NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

COMPUTER NETWORK OPERATIONS METHODOLOGY

by

Juan Carlos Vega

March 2004

Thesis Co-Advisors: Chris Eagle
Dan C. Boger

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** March 2004	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE Computer Network Operations Methodology			**5. FUNDING NUMBERS**
6. AUTHOR(S) Juan Carlos Vega			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) SPAWAR San Diego			**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE**
13. ABSTRACT (maximum 200 words) All nations face increasing tension between exploiting Computer Network Operations (CNO) in the military sphere and protecting the global information grid. The United States is moving apace to develop doctrines and capabilities that will allow them to exploit cyberspace for military advantage. Within the broad rubric of Information Operations, there is increasing effort devoted to integrating CNO into routine military planning. At the same time, these nations are becoming increasingly concerned at the dependency of their militaries, governments, economies and societies on the networked information systems that are emerging as the central nervous systems of post-industrial society. The armed forces desire to exploit and use CNO to their advantage is the central argument for this developed concept. This new weapons platform, or CNO, can be clearly identified so that the leaders will have an understanding of terms, limitations and capabilities of cyber operations. A methodology incorporating doctrine can be created to identify the Rules of Engagement (ROE) as well as the CNO components. The CNO area of operations and area of interest reach far beyond the typical battle space. The battle space has evolved and has penetrated every element of military operations that utilize computers and networks.			
14. SUBJECT TERMS CARVER, CNO, CNA, CNE, Computer Network Operations, Computer Network Attack, Computer Network Exploitation, Computer Network Defense, Cyber Warfare, Cyberspace, MDMP, Military Decision Making Process			**15. NUMBER OF PAGES** 109
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

COMPUTER NETWORK OPERATIONS METHODOLOGY

Juan Carlos Vega
Captain (Promotable), United States Army
B.A., California State Polytechnic University, Pomona, 1993

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 2004

Author: Juan Carlos Vega

Approved by: Chris Eagle
Thesis Co-Advisor

Dan C. Boger
Thesis Co-Advisor

Dan C. Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

All nations face increasing tension between exploiting Computer Network Operations (CNO) in the military sphere and protecting the global information grid. The United States is moving apace to develop doctrines and capabilities that will allow them to exploit cyberspace for military advantage. Within the broad rubric of Information Operations, there is increasing effort devoted to integrating CNO into routine military planning. At the same time, these nations are becoming increasingly concerned at the dependency of their militaries, governments, economies and societies on the networked information systems that are emerging as the central nervous systems of post-industrial society. The armed forces desire to exploit and use CNO to their advantage is the central argument for this developed concept. This new weapons platform, or CNO, can be clearly identified so that the leaders will have an understanding of terms, limitations and capabilities of cyber operations. A methodology incorporating doctrine can be created to identify the Rules of Engagement (ROE) as well as the CNO components. The CNO area of operations and area of interest reach far beyond the typical battle space. The battle space has evolved and has penetrated every element of military operations that utilize computers and networks.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

AI	Area of Interest
AIS	Automated Information System
AO	Area of Operation
ARP	Address Resolution Protocol
ATM	Asynchronous Transfer Mode
BDA	Bomb Damage Assessment
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
C2	Command and Control
C2W	Command and Control Warfare
C3	Command, Control, and Communication
C4ISR	Command, Control, Communication, Computers, Intelligence, Surveillance and Reconnaissance
CA	Collision Avoidance
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability
CCK	Complementary Code Keying
CDD	Capabilities Development Document
CIP	Critical infrastructure Protection
CNA	Computer Network Attack(s)
CND	Computer Network Defense
CNE	Computer Network Exploitation(s)
CNO	Computer Network Operation(s)
COA	Course(s) Of Action
COG	Center Of Gravity
COTS	Commercial Off The Shelf
CPD	Capabilities Production Document
CSLIP	Compressed Serial Link Internet Protocol
CSMA	Carrier Sense Multiple Access
DA	Direct Action
DFAS	Defense Finance and Accounting Service
DHCP	Dynamic Host Control Protocol
DHRA	Defense Human Resource Activity
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense information System Agency
DLA	Defense Logistics Agency
DNS	Domain Name System (or Service),

DoD	Department of Defense
DOTMLPF	Doctrine, Organizational, Training, Material, Leadership/Education, Personnel, and Facilities
DSSS	direct-sequence spread spectrum
ECAO	Enemy Course of Action
EPROM	Erasable Programmable Read Only Memory
FAA	Functional Area Analysis
FF	Fire and Forget
FHSS	Frequency-Hopping Spread Spectrum
FM	Field Manual
FNA	Functional Needs Analysis
FSA	Functional Solutions Analysis
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICD	Initial Capabilities Document
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IO	Information Operations
IOS	Inter-networking Operating System
IP	Internet Protocol
IPB	Intelligence Preparation of the Battlefield
IQ	Issue in Question
ISO	International Organization for Standardization
IW	Information Warfare
JCIDS	The Joint Capabilities Integration and Development System
JP	Joint Publication
LAN	Local Area Network
LLC	Logical Link Control
LOC	Lines Of Communications
MAC	Media Access Control
MDMP	Military Decision Making Process
MEDEVAC	Medical Evacuation
MIME	Multipurpose Internet Mail Extensions
MTU	Maximum Transmission Unit

NAI	Named Area of Interest
NATO	North Atlantic Treaty Organization
NCA	National Command Authority
NFS	Network File System
NMS	National Military Strategy
NSPD	National Presidential Directive
NSS	National Security Strategy
OASD	Office of Assistant Secretary of Defense
OFDM	Orthogonal Frequency Division Multiplexing
OPORD	Operations Order
OS	Operating System
OSI	Open Source Interconnection
OSPF	Open Shortest Path First
PAMO	Primary Area of Military Operations
PIA	Post Independent Analysis
POL	Petroleum, Oil, and Lubrication
PPP	Point-to-Point Protocol
PROM	Programmable Read Only Memory
RARP	Reverse Address Resolution Protocol
RE	Resultant Equities
REM	Resultant Equities Model
RET	Resultant Equities Threshold
RFI	Request For Information
RIP	Routing Information Protocol
ROE	Rules Of Engagement
ROM	Read Only Memory
SCADA	Supervisory Control And Data Acquisition
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SNMP	Simple Network Management Protocol
SOF	Special Operations Forces
SR	Special Reconnaissance
TCP	transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TOW	Tube Launched, Optically Tracked, Wire Guided
TST	Time-Sensitive Target

UDP	User Datagram Protocol
UM	Unit of Measure
US	United States
USACE	United States Army Corps of Engineers
USSTRATCOM	US Strategic Command
USTRANSCOM	US Transportation Command
WAN	Wide Area Network
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access

ACKNOWLEDGMENTS

My Family for their support and understanding

Beth Vega
Ryan, Brandon, Samantha

Those who labored through the words

Vickie Galante
Rhonda Menke
Nancy Sharrock
Elaine Pursel

Graciously signed on to assist my research at opportune times

Major Mark A. Givens, USMC
Lieutenant Commander Ramon O. Marin, USN
LCDR Paul Willey, USN
LT Bill Denton, USN
Kapitänleutnant Axel Schumann, FRG
LTJG Sean Kelley, USN

And those who shared their workspace, with or without permission

Cyber Risk Management Office (CRMO)

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

All nations face increasing tension between exploiting Computer Network Operations (CNO) in the military sphere and protecting the global information grid. The tension between these competing needs – one defensive and the other offensive – is the focal issue of this thesis. Led by the United States (US), North Atlantic Treaty Organization (NATO) nations are moving apace to develop doctrines and capabilities that will allow them to exploit cyberspace for military advantage. Within the broad rubric of Information Operations (IO), there is increasing effort devoted to integrating CNO into routine military planning. At the same time, these nations are becoming increasingly concerned at the dependency of their militaries, governments, economies and societies on the networked information systems that are emerging as the central nervous systems of post-industrial society. They are taking a range of actions, both unilaterally and multilaterally, to mitigate the resultant risks[1]. That the armed forces desire to exploit and use CNO to their advantage is the central argument for this developed concept.

Wars are fought on various fronts. The United States and her allies must use all resources at their disposal, including but not limited to: political, economic, military, and information operations. According to the National Security Strategy (NSS), our priority will be first to disrupt and destroy (adversarial) organizations of global reach, and to attack their leadership: command, control, and communications; material support; and finances. This will have a disabling effect upon the (adversaries') ability to plan and operate[2].

The National Military Strategy (NMS) is derived from the National Security Strategy, and is the role that the Department of Defense (DoD) will play in support of the NSS. It is crucial that DoD identify a methodology for classifying the components of

[1] Rathmell, Andrew Dr., Strategic and Organizational and Implications for Euro-Atlantic Security of Information Operations. [http://www.nato.int/acad/fellow/99-01/rathmell.pdf] December 2003.

[2] Bush, George, National Security Strategy, September 17, 2002, p. 5, [http://www.whitehouse.gov/nsc/nssall.html] September 2003.

CNOs and how they can be used as weapons. Such methodologies provide methods available to attack, exploit and defend cyber infrastructure. President Bush has signed a secret directive[3] ordering the government to develop, for the first time, national-level guidance for determining when and how the United States would launch cyber-attacks against enemy computer networks[4]. This new offensive and defensive weapons platform, or CNO, can be clearly identified so that the leaders will have an understanding of terms, limitations and capabilities of cyber operations. Thus, targets can be identified and universal terms established before commencement of operations. A methodology incorporating doctrine can be created to identify the Rules of Engagement (ROE) as well as the CNO components. The CNO area of operations and area of interest reach far beyond the typical battle space. The battle space has evolved and has penetrated every element of military operations that utilize computers and networks. When the cyber threats or objectives are identified, the target lists and components in CNO can be compiled. This type of standing list of cyber targets and their components will allow the decision makers to act promptly and effectively. Identifying causes and effects of a cyber attack will assist leaders to decide when and how to launch a cyber attack. This paper proposes a methodology that provides a decision support system utilizing CNO as part of conventional operations.

[3] Bradley Graham, "Bush Orders Guidelines for Cyber-Warfare," Washington Post, 7 February 2003: [http://www.washingtonpost.com/ac2/wp-dyn/A38110-2003Feb6?language=printer] February 2003.

[4] Ibid.

II. BACKGROUND

The DoD is grappling with decisions concerning the effective employment of Computer Network Operations (CNO). Such decisions demand a good understanding of this new strategy.

CNO has many definitions. It is used as a synonym for information warfare (IW), computer network attack (CNA), and/or a component of information operations (IO). These operations, offensive and defensive in nature, imply both exploiting the adversaries' systems and protecting one's own. CNO will be used to define military operations using computer technology and systems to disrupt, deny, degrade, or destroy resident information in computers and computer networks, or the computer networks themselves[5] in either peace or wartime environments. Interconnected computer systems are commonly referred to as a network, which is usually part of an infrastructure. These operations, offensive and defensive in nature, imply both exploiting the adversaries' systems and protecting one's own. The present state of CNO may be compared to that of the longbow prior to the battle of Crécy in 1346. The longbow, a hand-drawn wooden bow held vertically and used by medieval English archers[6], had already been invented and utilized in battle. It was the employment of the two centuries old weapon by the English, led by Edward the III, which proved decisive against the larger French forces[7]. It was the utilization of an existing weapon in a manner that made use of its overwhelming capabilities. Computer technology has evolved to the point that its utilization as a weapon is emerging.

---

[5] *Joint Doctrine for Information Operations, Joint Publication 3-13*, 9 October 1998, p. I-9, [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf] January 2004.

[6] Longbow, [http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=longbow&x=21&y=19] December 2003.

[7] Sullivan, Gordon R. and Harper, Michael V. *Hope Is Not A Metod* (New York, Broadway Books, 1996), p. 10.

The need adapt and develop a methodology for CNO has been thrust on DoD. The technology exists; anyone with a computer and knowledge of its capabilities can exploit this technology. The tasks at hand are how to use the new weapon to gain an advantage over our adversaries and simultaneously to create a defense in depth. Gen Gordon R. Sullivan and Michael V. Harper in "Hope is Not a Method," describe the Army's catalyst for change during the 1980's and 1990's. The end of the Cold War[8] forced the armed forces to adapt to a new environment. The Army was not prepared, it failed to predict, anticipate or plan for this change. At the time, the fall of the Berlin Wall was incomprehensible, coupled with the Panama invasion and Desert Shield/Storm, the Army was ill prepared to manage the monumental change. The Army had to change given the external factors, the collapse of the "Evil Empire". Today the DoD must also change, given the advent of CNO. Failing to act would allow adversaries to use the technology against our infrastructures and to overcome our superior weapons, similar to the English use of the longbow against the French.

The DoD is at the dawn of CNO, a new dimension of warfare. Private industry is now the leader in computer technological applications and systems. The applications are imperfect. These imperfections lead to vulnerabilities. These vulnerabilities are a design flaw, implementation error: omissions left in place unintentionally, programming errors that have remained undetected prior to distribution. Vulnerabilities may be malicious and non-malicious. These vulnerabilities can be exploited to gain advantage against an adversary. These systems are intertwined and connected to infrastructures that span far beyond the castle walls and create a new battle space.

[8] Ibid., p. 3-6.

III. THE BATTLE SPACE FOR CNO

Cyberspace is the new military operations frontier. To "deny enemy leaders the means of conducting military operations and controlling their nations (or organizations)"[9] should be a national objective for the war in cyberspace. Computer Network Operations (CNO) are information operations that aim to destroy, disrupt, deny and degrade enemy operations. There are two components and a third ancillary role to CNO. Computer Network Attack (CNA) and Computer Network Exploitation (CNE) are its main components. The necessary supporting role is Computer Network Defense (CND). Understanding and practicing CND sheds light on the capabilities of CNA and CNE.

The focus of CND is the defense of critical information and the systems that make up the information infrastructure commonly referred to as cyberspace. Computer network defense is the act of: "deterring, preventing, protecting, detecting, recovering, restoring, and responding."[10] What is the military defending? Is the military defending nuclear weapons or the commissary? A security breach of one can end the world, another will merely sound like the end of the world[11]. For the purpose of this paper, the United States is defending both and neither. On one hand, the United States is defending the information infrastructure that permits all military operations to function effectively and efficiently. The amount of resources dedicated to the information infrastructure is determined by security needs commensurate with the level of risk[12]. This paper will focus on the offensive aspects of CNO. The defense of friendly computer networks is important because of US dependence on information. Although the components of the defense of one's information infrastructure are the similar in CNO, the significant task of how to defend against an attack will not be addressed in this paper.

---

[9] Rand, The Joint Mission Framework *Intelligence Preparation of the Battlefield: An Overview*, p. 61, [www.rand.org/publications/mr/mr1287/mr1287.ch2.pdf] September 2003.

[10] Denning, Dorothy Lecture, Naval Postgraduate School, September 2003.

[11] Wadlow, T. A. (2000). The Process of Network Security. Addison Wesley: Reading, Massachusetts, p. 1.

[12] Government Information Security Reform, p. 2, [http://csrc.nist.gov/policies/Subtitle-G2.pdf], September 2003.

Computer Network Operations is a weapon that can either be classified as the main effort or a supporting role in a conventional military operation. CNO must be employed methodically to ensure that decision makers receive accurate and timely information. Given this accurate and timely information, the decision maker can determine the best course of action and can then mitigate the risk. This thesis addresses the role of CNO and how it could be methodically employed as part of a holistic approach to military operations. CNA and CNE are independent and conflicting operations when they share the same time and space continuum. The goal of CNA is to deny, degrade, destroy or disrupt a machine's ability to function as an information conduit. The goal of CNE is to gather, manipulate or interject information being passed by the machines. CNA is inconsistent with CNE. Controls must be established to ensure target de-confliction. Once an objective is identified, the decision-maker must decide whether CNO is part of the operation, or "is" the operation.

Existing methodologies for target analysis and hacking, combined, can be used to inform decision makers. The CARVER and Schmitt analysis are methodologies which, when used together, can provide the decision maker the information necessary to make an informed decision of Attack, Exploit or bypass a target. The CARVER system is used for target analysis and vulnerability assessment. The proposed methodology is a systematic approach that identifies the gathering of information for exploiting and/or attacking a cyber target.

It is important to follow a methodology because it is possible to miss key pieces of information related to a specific technology or organization.[13] CARVER and Schmitt analysis are complementary. CARVER identifies key, important elements that need to be addressed during an operation. Schmitt analysis identifies accountability and timing

[13] McClure, Stuart, Scambray, Joel and Kurtz, George, Hacking Exposed, Network Security Secrets & Solutions, Third Edition, Osborne/McGraw-Hill, 2001, p. 4.

issues that feed information into a methodology. A methodology feeds information to the decision maker and "must be horizontally integrated across strategic, operational, and tactical levels"[14].

Controlling the environment in which the enemy operates through CNO is a main cyberspace strategy goal. CND will be a major area for the US strategy. While the United States puts its effort into offensive CNO, CNA and CNE, the United States must also protect itself from attack. As US strategy is implemented, tactics and procedures for CNO are monitored by adversaries who can use these activities against the United States and its interests. CND is the active defense of information systems and extends beyond Operational Security (OPSEC) concerns.

The commander's strategy for military operations should use all available resources to limit an adversaries' freedom of operation. The commander needs to coordinate CNO with conventional strategy for in the conduct of military operations. The main effort of the US cyber strategy will be to use CARVER and Schmitt to identify the targets and their vulnerabilities for CNE and CNA. While conducting CNO, it should always be one step ahead with CND. CNO operates in cyberspace and targets the information that flows through the network. Cyberspace is used to transmit and receive information.

> Information is the soul of morale in combat and the balancing force in successful tactics. Yet in an era of warfare which is on the whole extremely enlightened, when we are so concerned for the welfare of troops that we strain our supply so that fresh eggs and oranges may be served in the front line during the course of the most rapid advance by field armies in history (Germany, April-May, 1945), we have not found the means to assure an abundant flow of that most vital of all combat commodities - information[15].

---

[14] National Defense University (NDU), Information Operations, the Hard Reality of Soft Power, p. 39, [http://www.jfsc.ndu.edu/schools_programs/jciws/iw/io_textbook.pdf] September 2003.

[15] Marshall, S. L. A. (1978). Men Against Fire: The Problem of Battle Command in Future War, p. 92, Gloucester, Massachusetts: Peter Smith.

Today, unlike the Second World War (WWII), the United States has ready access to information, and time expected for message delivery is measured in milliseconds. With computers and computer systems, information can be relayed along the chain of command in the blink of an eye.

IV. PROJECT BASELINE – DEFINED

It is important to understand the technology. There is a potential disconnect in the terminology between cyber operations and conventional operations. Current conventional operational terms can be used to define cyber warfare and can increase the understanding of the complexity of this new multifaceted means of war. We need an easily understood, standard terminology that is incorporated into joint doctrine. All agencies must have a common dictionary of terms regarding the breadth of information operations. This mutual understanding of concepts and terms applied to cyber operations will permit battlefield commanders to employ cyber warfare effectively across the expansiveness of the battlefield. This same understanding of cyber operations can be utilized in a deliberate defense against an attack on friendly assets.

The weapons of cyberspace are 1's and 0's, used to disrupt and cause a system to do destructive operations on behalf of an attacker. The attacker uses this tool to gain advantage over the adversary. Attacks can be classified as covert or overt. Most attacks can be conducted in a manner that either discloses to the victim that he is under attack or cloak the attack as a non-malicious problem. A disruption to the operations of a computer network will highlight this point. The cause of the computer network disruption can either be a missile strike (overt) or corruption of the address resolution protocol in a router (covert if done properly). Both can cause the desired effect, disruption in service. One is obvious while the other, not as clear, may be dealt with as a simple computer glitch. The ultimate goal of any attack is to force the adversary to act or react in manner that serves the attacker's objectives. The attacker is trying to get a desired action from the adversary. Selecting the target(s) that will best achieve the desired reaction is essential to the mission's success. It is necessary to understand the capabilities of the target so commanders can direct the operation with precision and confidence.

A. DESCRIPTION OF COMPUTER NETWORK OPERATIONS (CNO)

Computer network operations are part of information operations (IO) and information warfare (IW). IO is similar to IW operations conducted during non-wartime situations.

> Information warfare is the action taken to achieve information superiority by affecting an adversary's information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems and computer-based networks.[16]

Computer Network Operations are maturing to become one of the core competencies of IO/IW. CNO is the use of computer information systems to attack and exploit adversary information, information-based processes, information systems, and computer-based networks. The means of the operation is what distinguishes CNO from other operations. A computer network can be destroyed by means of kinetic energy or electro-magnetic pulse; a CNO utilizes hardware and software programs to achieve its desired effects. CNOs can also be used to defend one's own information, information-based processes, information systems and computer-based networks. This constitutes a computer network defense. In short, CNOs is defined as the use of computer systems to conduct military operations on the battlefield.

Successful CNO deployments depend on intelligence and preparation tailored to the situation at hand. Intelligence Preparation of the Battlefield (IPB) is a method of collecting, organizing, and processing intelligence.[17] In order to ensure effective CNO, the following steps are performed prior to an operation.

---

[16] DOD Information Operations Roadmap, 30 October 2003, [http://www.iwar.org.uk/iwar/] November 2003.

[17] Rand, The Joint Mission Framework *Intelligence Preparation of the Battlefield: An Overview*, p. 7, [http://www.rand.org/publications/MR/MR1287/MR1287.ch1.pdf] September 2003.

- Perform network reconnaissance against the target system.
- Map attributes such as operating system, architecture, and specific versions of listening services to known vulnerabilities and exploits.
- Perform target acquisition by identifying and selecting key systems.
- Enumerate and prioritize potential points of entry.

B. EXPLANATION OF TYPES OF ATTACKS

Computer Network Attacks (CNA's) are designed to deny, disrupt, degrade, or destroy either the information in computer and computer networks, or the computers and networks themselves[18]. CNA's are usually focused on attacking the confidentiality, integrity, and availability of information. CNA's are identified by their intentions within the mission. The following sections describe the four main types of CNA attack.

Deny - The purpose of this attack is to deny access to information. CNA's that deny access to information come in various forms. One of the most common of these is a Denial of Service (DOS) attack, which focuses on denying availability of information to authorized users for a specific time. A denial attack has the desired effect of preventing authorized users from accessing information by means of their computer information systems.

Disrupt - This type of attack focuses on disrupting as "attackers might surreptitiously reprogram enemy computers to disrupt the processes they control"[19]. The following elaborates on the purpose of a disruption attack. Denying electricity to an area by reprogramming the computers that control distribution within the power grid. A disruption attack introduces disorder and inhibits the effective utilization of information on the computer information systems.

[18] Bayles, William J. , The Ethics of Computer Network Attack, [http://www.totse.com/en/hack/legalities_of_hacking/excerpt4.html] September 2003

[19] Ibid.

Degrade - The purpose of this type of attack is to reduce the throughput of information, in an effort that "forces the enemy to use less efficient communications and processing means, slowing his logistics and decision cycles"[20] similar to use of conventional obstacles on a battlefield. A degradation attack creates latency in a system and can be used to channel information through more vulnerable systems. The attacker can take advantage of channalizations by directing or leading the adversary into the desired battle space. The desired battle space can be the use of a more vulnerable medium. It does not have to be network-related (e.g., unsecured telephone or radio transmission). This attack can support the exploitation of a computer system.

Destroy - As the name implies, this attack is the most forceful. Kinetic munitions could be used to accomplish this, but kinetic munitions are conventional means of engaging targets and not CNA. Instead, a CNA destruction attack involves viruses and/or other malicious programs to destroy computer networks and associated software and hardware components.

C. COMPUTER NETWORK EXPLOITATION

Computer Network Exploitation (CNE) is the collection of intelligence and enabling operations in order to gather data from target adversary automated information systems (AIS) or networks[21]. CNE, the 2nd pillar of CNO, is the gathering and manipulation of information. This information is used to enhance the friendly elements observation of the battlefield while obscuring that of the target. John Boyd's [United States Air Force (Retired)] decision cycle model reflects the importance of information in the decision making capabilities of allies and adversaries. Command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) are the targets of CNE. Information is the goal; taking advantage of the media is the means.

[20] Ibid.

[21] United States Joint Forces Command, [http://www.jfcom.mil/about/glossary.htm] September 2003.

CNE is the deliberate act of infiltrating an adversary's information systems to affect the decision-making capabilities of the target adversely and enhancing intelligence of friendly elements. COL(R) Boyd's Observation, Orientation, Decision and Action cycle (OODA Loop) focuses on affecting the decision maker's ability to act decisively in the right time and space. By having control of the adversary's OODA loop, the friendly elements can gain decision superiority. Decision superiority is the ability of the allied commander - based upon information superiority and situational understanding - to make effective decisions more rapidly than the adversary, thereby allowing one to dramatically increase the pace, coherence, and effectiveness of operations[22]. CNE allows the allied commander to extract intelligence information from the target system's network that can enhance the capabilities of current and future operations. CNE also allows the allied commander to inject information that degrades the adversary's abilities to observe the battle space properly. Extraction and injection are defined as follows:

- **Extraction** - Extracting information is the act of capturing data streams transiting a network or gaining access to target-resident files. Access to the links and nodes of the network topology is necessary to gain the information. The assets gathered from the exploitation are processed, analyzed, integrated and interpreted to determine the state of the adversary's orientation. Information and knowledge about an adversary, obtained through the observation of the information stored on the adversary's computers, can be used to the advantage of the allied commanders. The intelligence gathered from this extraction of data can then be utilized to return to a target and inject information. This is a passive (listening) technique.
- **Injection** - This involves injecting data streams or files in manipulation of the adversary's information. This injection gives the friendly commander the ability to manipulate the information, thus distorting an adversary's perception or observation of the battle space, to the advantage of the allied commander. This is an active (modifying) technique.

Attaching to a network can be accomplished physically or through cyberspace. The links and nodes to be targeted must be within an adversary's trusted network. The trusted network is assumed to contain valid and credible information by the adversary. Attaching to a network using physical means is done by introducing hardware and/or

[22] Ibid.

software that has the capability of gathering and storing data for use by the allied commander. Attaching to a network through cyberspace is gaining unauthorized access to the network external to the trusted infrastructure.

Control the information, then you control the battle space. By attacking and/or exploiting the information on an adversary's computer network, the commander can then control the enemy's OODA loop and can thus influence the success of allied operations. Attacks and exploits are the "what" in the phrase "Who, what, where, when and why?" The "why" is to gain decision superiority. "What" are you going to attack and exploit? "What" are you going to target?

V. THE TARGETS

A. GENERAL DESCRIPTION OF CNO TARGETS

The targets of CNO are the pertinent information systems that the adversary utilizes to assist in making decisions. These systems are networks comprised of hardware and software. "Cyberspace is the information space consisting of the sum total of all computer networks"[23]. In order to prepare for an attack and to engage the target effectively, a description of the hardware and software must be acquired. The following section describes hardware, software and configurations that can be targeted.

1. Hardware

Computer network hardware is essentially any physical component that has connectivity to a network and processes or passes information to another component or to the end user. The hardware can be a computer, but it is not limited to that (Figure 1). Hardware is typically a nodal point of a network topology. Examples of nodal platforms that can be targeted are computers, peripheral devices, networking devices, and servers.

- **Computer –** A computer is a programmable machine that can respond to specific set of instructions and can execute programs[24]. A computer consists of memory, central processing unit, mass storage device and peripheral devices. A computer is hardware that can be setup in a myriad of configurations. Performance and mobility are influenced by size, design, and processing power. The general choice of the platform is a question of functionality and the purpose to be achieved. Computers, like most hardware devices, have configurable software that runs the system.
- **Peripheral devices –** A peripheral device is not part of the essential computer. These components are both internal and external devices, and include printers, monitors, disk drives, scanners and other input/output devices. The software that controls peripheral devices is called a driver.
- **Network Device –** A network device is a machine that passes information between computers. Common network devices are routers, switches, and hubs. A network device forwards data along the network. The network device has a series of rules or communication protocols that specify how packet headers are formed and how packets are processed. The set of

[23] Denning, D. E. (1999). Information Warfare and Security. Georgetown University: Addison-Wesley, Boston, p. 22.

[24] [Webopedia.com] February 2003.

protocols used for the Internet are named TCP/IP after the two most important protocols in the set: the Transmission Control Protocol and the Internet Protocol. Hardware devices that connect networks in the Internet are called IP routers because they follow the IP protocol when forwarding packets. A router examines the header in each packet that arrives to determine the packet's destination. The router either delivers the packet to the destination computer across a local network or forwards the packet to another router closer to the final destination. Thus, a packet travels from router to router as it passes through the Internet. Similar devices to routers are switches, hubs and devices that, when configured, can behave like a device with lower capabilities.

- **Servers –** A server is a computer that allocates resources on a network. A server can manage resources for other computers. The physical characteristics of a server are similar to those of a computer but differ in function[25]. A Server is a computer running administrative software that controls access to all or part of the network and its resources. A computer acting as a server makes resources available to computers acting as clients on the network. There is no specific way to penetrate a server since there are uncounted possibilities

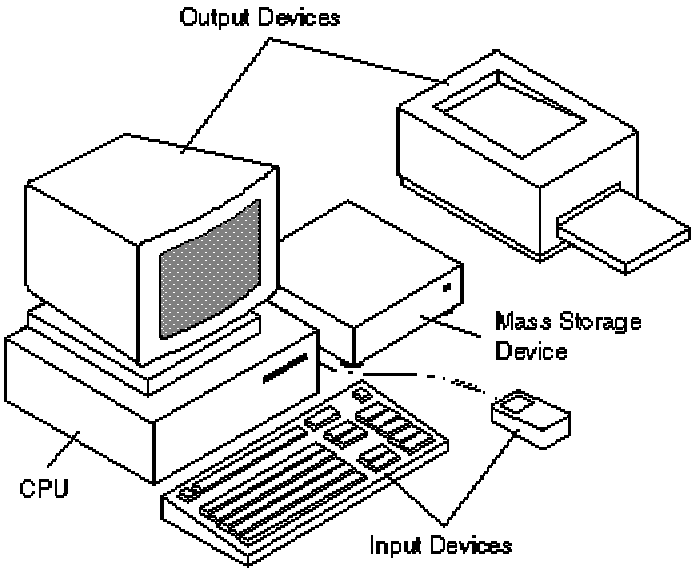


Figure 1. Computer Hardware Examples

The second set of components in a computer network are the links. The links are hardware or means by which data is passed from one nodal device to another. A link

[25] Ibid.

connects nodes (Figure 2). The actual connections to the hardware are one of many peripheral devices designed to accommodate the specific type of means used by the link. The link is characterized by medium, protocol, throughput and maximum distance between two nodes. The media can be a wires, radio waves, or optical connections. Common media include fiber optics, coax copper wire and radio frequencies (RF). A protocol, such as Ethernet, is an agreed-upon format for transmitting data between two devices[26]. Protocols can be, but are not always, media-specific, e.g., RF Wireless protocols (Table 1), yet share some commonality.

Network link and Nodal Topology

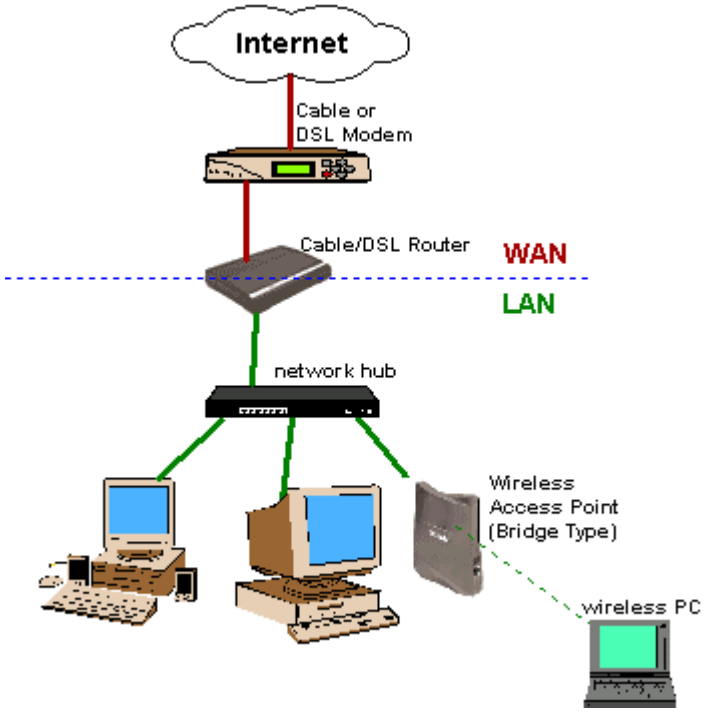


Figure 2. ---- — — Links and Nodes (Devices)

[26] Ibid.

Table 1. Wireless Designations[27]

Standard	Data Rate	Modulation Scheme	Security	Pros/Cons
IEEE 802.11	Up to 2Mbps in the 2.4GHz band	FHSS or DSSS	WEP & WPA	This specification has been extended into 802.11b.
IEEE 802.11a (Wi-Fi)	Up to 54Mbps in the 5GHz band	OFDM	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Eight available channels. Less potential for RF interference than 802.11b and 802.11g. Better than 802.11b at supporting multimedia voice, video and large-image applications in densely populated user environments. Relatively shorter range than 802.11b. Not interoperable with 802.11b.
IEEE 802.11b (Wi-Fi)	Up to 11Mbps in the 2.4GHz band	DSSS with CCK	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." Not interoperable with 802.11a. Requires fewer access points than 802.11a for coverage of large areas. Offers high-speed access to data at up to 300 feet from base station. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
IEEE 802.11g (Wi-Fi)	Up to 54Mbps in the 2.4GHz band	OFDM above 20Mbps, DSSS with CCK below 20Mbps	WEP & WPA	Products that adhere to this standard are considered "Wi-Fi Certified." May replace 802.11b. Improved security enhancements over 802.11. Compatible with 802.11b. 14 channels available in the 2.4GHz band (only 11 of which can be used in the U.S. due to FCC regulations) with only three non-overlapping channels.
Bluetooth	Up to 2Mbps in the 2.45GHz band	FHSS	PPTP, SSL or VPN	No native support for IP, so it does not support TCP/IP and wireless LAN applications well. Not originally created to support wireless LANs. Best suited for connecting PDAs, cell phones and PCs in short intervals.
HomeRF	Up to 10Mbps in the 2.4GHZ band	FHSS	Independent network IP addresses for each network. Data is sent with a 56-bit encryption algorithm.	**Note:** HomeRF is no longer being supported by any vendors or working groups. Intended for use in homes, not enterprises. Range is only 150 feet from base station. Relatively inexpensive to set up and maintain. Voice quality is always good because it continuously reserves a chunk of bandwidth for voice services. Responds well to interference because of frequency-hopping modulation.
HiperLAN/1 (Europe)	Up to 20Mbps in the 5GHz band	CSMA/CA	Per-session encryption and individual authentication.	Only in Europe. HiperLAN is totally ad-hoc, requiring no configuration and no central controller. Doesn't provide real isochronous services. Relatively expensive to operate and maintain. No guarantee of bandwidth.
HiperLAN/2 (Europe)	Up to 54Mbps in the 5GHz band	OFDM	Strong security features with support for individual authentication and per-session encryption keys.	Only in Europe. Designed to carry ATM cells, IP packets, Firewire packets (IEEE 1394) and digital voice (from cellular phones). Better quality of service than HiperLAN/1 and guarantees bandwidth.

[27] Ibid.

Within theses standards, there exist several sub-designations, such as wireless, Simple Network Management (SNMP), Internet (IP) and its subsets Internet Control Message Protocol (ICMP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), File Transfer (FTP), Hyper Text Transfer (HTTP), HTTP Secure (HTTPS), and Dynamic Host Control (DHCP) protocols. Vulnerabilities can be exploited at every level of the Open Source Interconnect model depending on the protocol that is being used.

> The Open System Interconnection (OSI) model defines a networking framework for implementing protocols in seven layers. Control is passed from one layer to the next, starting at the application layer in one station, proceeding to the bottom layer, over the channel to the next station and back up the hierarchy.[28]

By understanding the software application the attacker can isolate the vulnerabilities that lead to a successful attack. Information is passed through the OSI stack from one device to another with a link that connects at the physical layers, Figure 3. Each of the seven layers has a specific function and utilizes specific programs or software and different protocols, Table 2.

[28] Ibid.

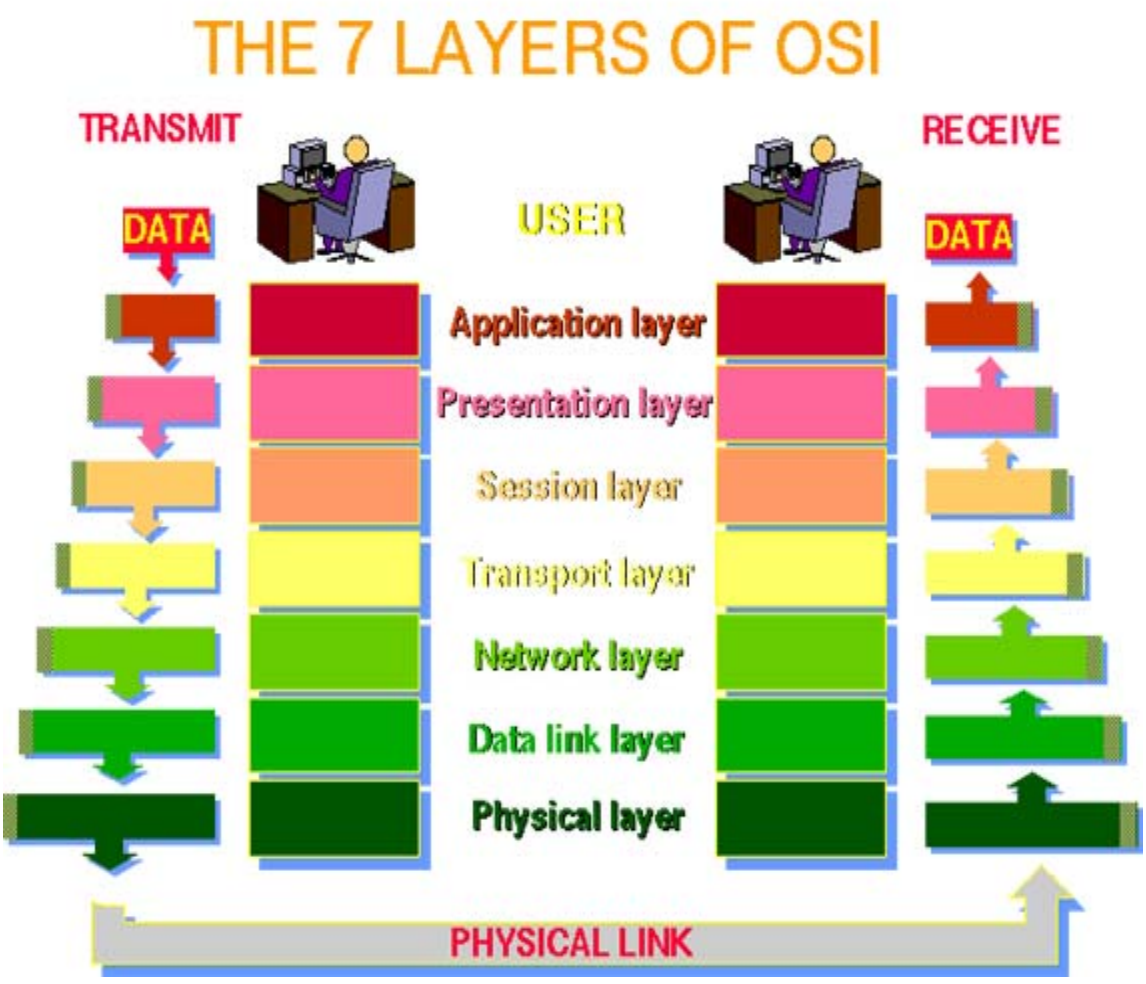


Figure 3. Layers of OSI

Table 2. OSI Model[29]

ISO-OSI Model		
Layer	**Function**	**Protocol**
Application (Layer 7)	This layer supports application and end-user processes. Communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified. Everything at this layer is application-specific. This layer provides application services for file transfers, e-mail, and other network software services. Telnet and FTP are applications that exist entirely in the application level. Tiered application architectures are part of this layer.	DNS, TFTP, BOOTP, SNMP, RLOGIN, FTP, SMTP, MIME, NFS, FINGER
Presentation (Layer 6)	This layer provides independence from differences in data representation (e.g., encryption) by translating from application to network format, and vice versa. The presentation layer works to transform data into the form that the application layer can accept. This layer formats and encrypts data to be sent across a network, providing freedom from compatibility problems. It is sometimes called the syntax layer.	Null
Session (Layer 5)	This layer establishes, manages and terminates connections between applications. The session layer sets up, coordinates, and terminates conversations, exchanges, and dialogues between the applications at each end. It deals with session and connection coordination.	Null
Transport (Layer 4)	This layer provides transparent transfer of data between end systems, or hosts, and is responsible for end-to-end error recovery and flow control. It ensures complete data transfer.	TCP, UDP
Network (Layer 3)	This layer provides switching and routing technologies, creating logical paths, known as virtual circuits, for transmitting data from node to node. Routing and forwarding are functions of this layer, as well as addressing, internetworking, error handling, congestion control and packet sequencing.	IP, ARP, RARP, ICMP, RIP, OSPF, BGP, IGMP
Data Link (Layer 2)	At this layer, data packets are encoded and decoded into bits. It furnishes transmission protocol knowledge and management and handles errors in the physical layer, flow control and frame synchronization. The data link layer is divided into two sublayers: The Media Access Control (MAC) layer and the Logical Link Control (LLC) layer. The MAC sublayer controls how a computer on the network gains access to the data and permission to transmit it. The LLC layer controls frame synchronization, flow control and error checking.	SLIP, CSLIP, PPP, MTU
Physical (Layer 1)	This layer conveys the bit stream - electrical impulse, light or radio signal -- through the network at the electrical and mechanical level. It provides the hardware means of sending and receiving data on a carrier, including defining cables, cards and physical aspects. Fast Ethernet, RS232, and ATM are protocols with physical layer components.	ISO 2110, IEEE 802, IEEE 802.2

[29] Ibid.

Some protocols are layered when more than one protocol is in use. Layered protocol implies that during a transmission of information, more than one protocol may be used. Each designation may have its own type of peripheral device to connect the hardware. Other common standards are Infrared Data Association (IrDA), a group of device manufacturers that developed a standard for transmitting data via infrared light waves and fiber optic, a technology that uses glass (or plastic) threads (fibers) to transmit data[30].

One must also consider the possibility that some attacker might be successful in having the adversary execute the malicious code or attack for him. This is done by utilizing a Trojan Horse. A Trojan horse is "a program that purports to be a useful tool but actually installs malicious or damaging software behind the scenes"[31]. On execution, this software will open a back door for the attacker, allowing him to control the machine. A Trojan horse masquerades as a desired application while executing a destructive program

2. Software

Software is the program that controls the hardware. All hardware has software associated with its operation. There are generally two types of software, system and application software.

1. System software refers to the operating system and all utility programs that manage computer resources at a low level. Non-O/S systems software includes compilers, loaders, linkers, and debuggers.[32]

2. Applications software comprises programs designed for the end user, and includes word processors, database systems, and spreadsheet programs.

---

[30] Ibid.

[31] McClure, Stuart, Scambray, Joel, Kurtz, George, Hacking Exposed, Network Security Secrets & Solutions, Third Edition, Osborne/McGraw-Hill, 2001, p. 123.

[32] [Webopedia.com] February 2003.

Many computers also contain an operating system (OS) as we all know e.g. Windows, MAC OS, UNIX or Linux. The operating systems are by far the most complex piece of software that run on a given system.

> Operating systems perform basic tasks, such as recognizing keyboard input, sending output to the display screen, keeping track of files and directories, and controlling peripheral devices such as disk drives and printers. For large systems, the operating system has even greater responsibilities and powers. Like a traffic cop, it makes sure that different programs and users running at the same time do not interfere with each other. The operating system is also responsible for security, ensuring that unauthorized users do not access the system.[33]

Due to the complexity of OS's, numerous vulnerabilities exist. The number of patches available for today's OS is growing exponentially due to the vulnerabilities and security holes exploited by hackers. A computer patch is temporary fix of an error or defect in software program.

The importance in understanding hardware and software lies in their vulnerabilities. Vulnerabilities exist in the software that runs on the computer networks. Computer networks are comprised of hardware and software. It is said that the most secure computers are those that are turned off. Computers that are part of a network are exposed to attack and exploitation if not configured properly and/or any one of the nodes and links is vulnerable. Information systems can be hardened, yet vulnerabilities still exist, remaining to be discovered or exploited. Hardware and software connects the internet, intranets, extranets, wide area networks, local area networks and therefore can be attacked. As an attacker hops along the chain he or she can exploit the systems by using flaws and vulnerabilities residing in the firmware, operating system, or running applications

Firmware is the most basic software that runs standalone systems like Switches or Wireless Access Points. It is not designed to be easily changed, but can be configured by

[33] Ibid.

a somewhat difficult process called flashing (the process of updating the firmware memory). Firmware is also referred to as ROMs, PROMs and EPROMs (variations of Read Only Memory).

A service is the interface that connects the data being transferred between computer transmissions. There are two broad categories of services, connectionless and connection-oriented. Connectionless services are analogous to a fire and forget (FF) missile system. In a connectionless system, a message is sent to the destination and no further action is required by the sender. The data being sent (the missile) must have coordinates of the destination and the message (the munitions). If the FF missile control is being passed or handed off to an enroute navigation system, the coordinates must be in a predetermined and agreed upon protocol or format for the hand-off to occur. The predetermined and agreed upon protocol or format is known as the addressing scheme. All the information is contained in the FF missile; there is no reach back for information to the launching platform. In a connection-oriented scenario, a stream of information is passed between sender and receiver, such as a Tube Launched, Optically Tracked, Wire Guided (TOW) Missile. With a TOW missile, bursts of data are sent between the missile and launcher. The data steam must be continuous or the TOW missile may not hit the intended target. When the connection is established, the passing of information is continuous until the transmission is terminated by either sender or receiver. Connectionless and connection-oriented are generic terms that incorporate many technologies and designs. It is sufficient to understand what type of service is being targeted.

As new operating systems are developed, the trend goes towards more security, but coding errors, incorrect functionality, poor design, and insecure default settings leave systems susceptible to new attack. In addition to the generic OS, the inter-networking OS, abbreviated IOS is a special operating system that runs networking devices like routers. Although the functionality is specifically tailored to the needs of the router and its remote control, it still can be either poorly configured or flawed. Especially when a

router is overtaken by an attacker it is difficult to determine the damage and to re-establish security. The questions in case of attack are how long did the attacker own the device? Did he reroute the traffic, filter the traffic or just enforce a denial of service? Further, there is the application itself that runs on the networked platform. Very well known applications are the internet browser or the email program. They might and do help an attacker to be successful by having flaws and security holes like OS's.

B. ATTACK VECTOR

1. General Description of a Vector

For every computer network operation there must be a vector to deliver the payload. The vector is equivalent to avenue of approach for conventional operations. A vector is the route of a CNO leading to its target or key position in relation to the targeted network. Attack vectors require both physical and cyberspace access. Access is virtually unlimited by location. The start point of the attack can occur on the battlefield, from a neighboring country or the United States, or a deployable platform from the sea, land, air, or space. The route of an attack is important for international implications and responsibilities.

2. Vector Flight Path

An attack vector is the route that successfully leads to the target. Attack vectors are literally the keys that allow payloads to be executed on the target[34]. The payload is the destructive program that will facilitate or execute an attack or exploitation. A payload is designed for a specific target to accomplish a desired effect. The vector used to deliver the payload is also specifically designed or utilized to support the desired effect. Vectors have limited life span, and are vulnerable because they take advantage of security holes on target networks. Security holes can be intentional and unintentional. Commanders use vectors to exploit security holes for unauthorized access to the target system. Once the vector is utilized and discovered, it can be closed. Many vectors are likely to be closed through normal system updates to operating systems, virus scans, firewall updates, intrusion detection systems, etc. Another factor that limits the utility of

[34] H. B. Gary, Phoenix Challenge Conference, July 2003, Gregg Hoglund, LLC.

a vector is when a rogue cracker exposes the vulnerability of a vector. A cracker is an individual or group whose sole aim is to gain unauthorized access to a system or utility from a program.

The start point of the vector can determine what type of vector is acceptable based on the rules of engagement. CNO vectors, arguably, can be construed as being subject to laws, national and international, similar to aircraft. A CNO vector is equivalent to an aircraft flight path. Just as the bomb an aircraft carries is the payload that will inflict physical damage, a CNO payload is the software or data component that exploits a known computer system vulnerability. The vectors must be directed to ensure compliance with existing laws or operational rules of engagement that are self imposed rules and guidelines which can be more restrictive than laws. Vectors that begin on the battlefield may require physical access to target systems or ancillary systems that can have trusted access to the target system.

Vectors have a limited utility. Repeated exposure can limit their usability when the adversary is able to patch the security hole effectively. Physical access is subject to similar time constraints if the vulnerability is discovered and secured. The most valuable systems vulnerabilities are zero-day exploits. A zero-day exploit is one that exists prior to the availability of any patches or mitigating techniques for the associated vulnerability. Any vulnerability, either poorly configured or unpatched system, is subject to exploitation - zero-day or otherwise - and must be closely managed to ensure the vector exists so that commanders can use it to accomplish its mission.

C. TARGETING CRITICAL INFRASTRUCTURE

1. Type of Target

The widespread usage of computers in the military and commercial sector has ensured technology dependency by both civilian and government entities. Technology transcends all sectors of a nation, including business, finance, educational, or military institutions. Such dependency has elevated technology to a strategic, operational and

tactical center of gravity. CNA's may be focused on either military or civilian targets, but in most cases will affect both. CNA's, like any other type of attack, may be used to influence politics or other types of events such as financial, social, or military[35].

2. Civilian Targets

Civilian targets include any infrastructure that supports the civilian population either directly or indirectly. Civilian infrastructure is owned by the public and private sector. Civilian targets are the focus when attacks are designed to "disrupt electricity supplies and telephone service, interfere with air traffic control, cause leaks or explosions at chemical plants or refineries, and cause economic damage," all in an effort to indirectly affect civilians[36].

The computer systems that operate civilian industrial infrastructure are known as SCADA systems. SCADA systems, supervisory control and data acquisition, are vulnerable targets because they are unique systems, not scrutinized by thousand of users and agencies as is Microsoft Windows. SCADA's are not upgraded with the same frequency as more heavily used software, due to complexity and expense. For instance, "The SCADA system used by the Manchester Power in New England was deployed in early 1970's and had not been substantially changed as of 1997"[37]. Exploits and vulnerabilities may remain in zero-day-exploit state for many years and make SCADA's opportunistic targets.

3. Military Targets

Military targets include infrastructure, software, hardware or data that influences Command and Control (C2), a part of Command and Control Warfare (C2W). Attacking

---

[35] Buettner, Raymond, Naval Postgraduate School, October 2002.

[36] Bayless, William J., The Ethics of Computer Network Attack, [http://www.totse.com/en/hack/legalities_of_hacking/excerpt4.html] September 2003.

[37] Rattray, Gregory J. Strategic Warfare in Cyberspace, The MIT Press, Massachusetts, 2001, p. 58.

and destroying such military targets results in degrading or destroying an adversary's ability to command and control forces, thus increasing "uncertainty of war for the adversary and a slowing of his decision cycle."[38]

4. Critical Infrastructure Defined

Those systems and assets essential to plan, mobilize, deploy, and sustain military operations and transition to post-conflict military operations, and whose loss or degradation jeopardize the ability of the Department of Defense to execute the National Military Strategy[39] .

> It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of minimal duration, and manageable, and cause the least damage possible. President George W. Bush[40]

DoD has an infrastructure that is interwoven with civilian infrastructure. The United States government has identified nine sectors of critical infrastructure. Military targets can be legitimate attack objectives as well as the civilian sector. The United States government has paired the civilian infrastructure with the DoD equivalent sector. The logic behind this pairing is that the safeguards of one can used to protect the other. An inference can also be made that a weakness in one may also be found in the other. The nine sectors and the civilian and their military counterparts are depicted in Table 3.

---

[38] Bayles, William J., The Ethics of Computer Network Attack, [http://www.totse.com/en/hack/legalities_of_hacking/excerpt4.html] September 2003.

[39] Joint Staff Definition used in coordinated response to Draft DoDD 8500.l, [http://www.dtic.mil/doctrine/index.html] November 2003.

[40] [http://www.whitehouse.gov/news/releases/2004/01/20040121-6.html] January 2004.

Civilian Sector	Military Sector
Financial Services	DFAS
Transportation	USTRANSCOM
Public Works	USACE
DII & C3	DISA
ISR	DI
Health Affairs	OASD, Health Affairs
Personnel	DHR
Space	USSTRATCOM
Logistics	DLA

Table 3. Nine Sectors and the Civilian and Their Military Counterparts

The depiction may give the impression that they are separate entities. In reality, Civilian and Military sectors share much of the same infrastructure. This infrastructure is vulnerable to CNO. The military infrastructure can be expected to maintain a high level of security and protection. The same conclusion cannot be assumed for the civilian sector. The focus of military organizations is to attack and defend. This philosophy can be carried over to computer networks. Although the actual implementation may vary by target, the concepts of attacking and defending information may not be new. On the other hand, the civilian sector is not motivated by military conflict. Here, motivations vary depending on the type of institution and its customer base. Some civilian institutions provide a service of availability such as the transportation sector. The pairing of the civilian and military sectors provides a military focus of security to the civilian sector, while providing the innovation and resources of the private sector to the military. In the transportation sector, for instance, guarding its automated rail and traffic systems is not its primary focus. As the period following the terrorist attacks of September 11, 2001 demonstrated, the state of California could not protect its key infrastructure, major bridges, causeways, and highways, without military assistance. The lesson to be learned from this is that a method of targeting the military information systems may be via its civilian counter part.

The military does not control its entire infrastructure. DoD is dependant on the civilian infrastructure with few exceptions. The functions that each of these sectors provide are categorized with the key responsibilities and missions that can be targeted. The military sectors are as follows:

- Defense Finance and Accounting Service (DFAS) fulfills the important fiscal responsibilities for the DoD.[41]
- US Transportation Command (USTRANSCOM) the single manager of the Defense Transportation System (DTS), comprised of American land, sea and air mobility assets. Coordinate enroute support of troops and equipment. USTRANSCOM moves troops and equipment through coordinated use of military and commercial transportation modes.[42]
- US Army Corps of Engineers (USACE) provides planning, designing, building and operating water resources and other civil works projects (Navigation, Flood Control, Environmental Protection, Disaster Response, etc.). Designing and managing the construction of military facilities for the Army and Air Force. (Military Construction) Providing design and construction management support for other Defense and federal agencies. (Interagency and International Services).[43]
- Defense Information System Agency (DISA) enables communications, joint command and control, defensive information operations, combat support computing, and joint interoperability support.[44]
- Defense Intelligence Agency (DIA) provides military intelligence to warfighters, defense policymakers and force planners, in the Department of Defense and the Intelligence Community, in support of U.S. military planning and operations and weapon systems acquisition.[45]
- Office of Assistant Secretary of Defense (OASD), Health's mission is to enhance DoD and our Nation's security by providing health support for the full range of military operations and sustaining the health of all those entrusted to our care.[46]
- Defense Human Resource Activity (DHRA) mission is to provide program support, information management, and administrative services to the DoD Components on human resource matters and to collect, archive and

41 [http://www.dfas.mil/] September 2003.

42 [http://www.transcom.mil/] September 2003.

43 [www.usace.army.mil/] September 2003.

44 [www.disa.mil/] September 2003.

45 [http://www.dia.mil/] September 2003.

46 [www.ha.osd.mil] September 2003.

provide management information, research and analysis of human resources and other related functional area data bases for the DoD.[47]

- US Strategic Command (USSTRATCOM) has the mission launching and operating satellites, supporting joint-service military forces worldwide with intelligence, communications, weather, navigation, and ballistic missile attack warning information, engaging adversaries from space and assuring U.S. access to, and operation in, space and denying enemies that same freedom.[48]
- Defense Logistic Agency (DLA) provides worldwide logistics support for the missions of the Military Departments and the Unified Combatant Commands under conditions of peace and war. It also provides logistics support to other DoD Components and certain Federal agencies, foreign governments, international organizations, and others as authorized.[49]

The military sector may be the target, but the vector of attack may begin in the civilian infrastructure that is can be less hardened and guarded. The bridge between the civilian and military infrastructure is likely found in the network. The risk associated with the infrastructure can be measured. By reverse engineering a risk model, the likely vector and payload can be determined.

D. SIMPLE RISK MODEL

Figure 4 depicts that criticality is determined according to the importance of contribution to the mission. Threat and vulnerability do not determine criticality[50].

- Determine what is most important; identify the critical infrastructure assets.
- Prioritize asset assessments based on the threat to critical assets, if specific threat information is available.
- Pick from the critical assets priority list to establish the vulnerability assessment work program.
- Evaluate risks from a mission perspective.

---

47 [www.dhra.osd.mil] September 2003.

48 [www.stratcom.af.mil] September 2003.

49 [www.dla.mil/] September 2003.

50 Office of the Secretary of Defense Critical Infrastructure Protection Program Compact Disc – 2002.

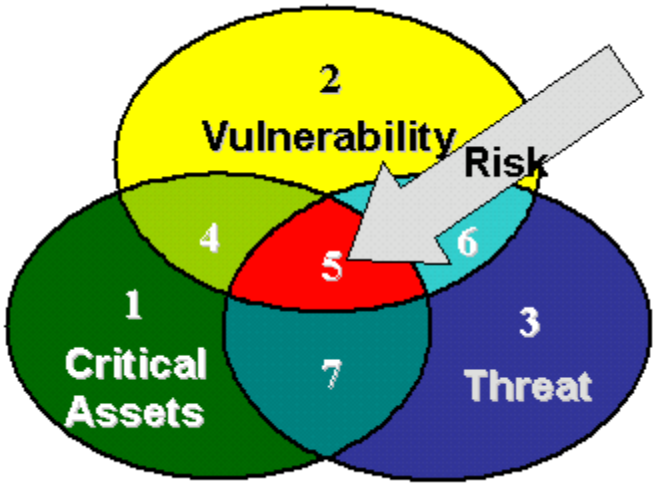


Figure 4. Determination of Criticality

Legend[51]

1 – Critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat exposure.
2 – Vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there is no known threat exposure.
3 – Threat environment for which there is no known threat to critical assets or access to vulnerabilities (or vulnerability information).
4 – Critical assets for which there are known vulnerabilities, but no known threat exposure.
5 – Critical assets for which there are known vulnerabilities and threat exposure.
6 – Threat has acquired specific knowledge and/or capability to exploit a vulnerability although not a critical asset vulnerability.
7 – Critical asset for which there are no known vulnerabilities, but there is exposure to a specific threat.

CNO's do not automatically discriminate between civilian or military infrastructure. This further complicates policy and tactical employment. Commanders need to control and limit collateral damage. Target coordination is necessary to ensure that deconfliction occurs in the battle space between conventional forces, CNA, and CNE operators. As the network-centric era of warfare progresses, it is incumbent upon military leaders to harness the energy of these weapons and use them to fight our nation's battles in an effective, efficient, informed, ethical, and lawful manner. It is incumbent on military planners to provide the systems to allow commanders to make the informed decisions.

An understanding of the complexity of networks and their function, commanders can recognize their vulnerabilities and exposure to threats. The targets can be military, civilian or dual use infrastructure. The vulnerabilities can be exploited to gain an advantage over an adversary. With this knowledge, a methodology can be developed to assist the commander in decision making. Controlling the information that the adversary observes and orientates, can ultimately influence the enemy's ability to decide and act.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. THE METHODOLOGY

A. WHAT IS A METHODOLOGY?

A methodology attempts to provide a mechanism for evaluating data and injecting knowledge to reach a reasonable conclusion. The way in which one discovers information; a methodology describes how something will be (or was) done. The methodology includes the methods, procedures, and techniques used to collect and analyze information[51]. A methodology is a systematic observation of events that provides commanders the understanding to make decisions and to act appropriately for the given situation or environment. The orientation and understanding of computer network operations varies between commanders.

The use of methodologies is widespread and done subconsciously to assist individuals in decision making. The processes that one utilizes to make everyday decisions are complex. Everyday decisions have many variables that are quickly sorted, ordered, valued or weighed and compared to arrive at something as simple as how to begin the day. That information is processed based on one's knowledge and experience. Where to eat breakfast is one example. The possibilities are numerous, and include preparing a hot meal vs. a cold meal in the home or eating at a restaurant: fast-food vs. dining in. Within these categories there are subcategories: the type of food available, time available for preparation and consumption and other even more subjective reasons, such as diet, likes or dislikes, how the food will interact with the afternoon or evening meals. Decisions like those described are made in seconds by individuals and the best outcome depends on the value placed on each aspect of the decision. The outcome will vary for most people based on their own experience, expectations and desires. The same question presented to a group is unlikely to be decided as efficiently as meeting the needs and desires of one individual. Couple the question with an unfamiliar or dynamic subject and the outcome is less clear then a familiar subject area. A methodology can improve

51 JP 3-05.5 Joint Special Operations Targeting and Mission Planning Procedures, [www.synergyaids.com/lacriaids/glossary.asp] August 1993.

the effectiveness and efficiency of the decision making process. By using an appropriate methodology, something as simple as "what is for breakfast?" can be used for problems more complex problems like "how to engage a hostile enemy force?"

The United States military uses methodologies to plan warfare. It uses methodologies to enable the comparison and categorization of different plans, capabilities and desired results. Two widespread methodologies include CARVER and the Military Decision Making Process (MDMP). A third methodology is the Schmitt Analysis that examines a measured response to Computer Network Operations (CNO) and the geopolitical and military ramifications. The objective is to combine these three different methodologies into one that can then be applied to a military decision support system.

B. CURRENT METHODOLOGIES

1. Military Decision Making Process

The Military Decision Making Process (MDMP) is used throughout the US Army to evaluate and compare courses of action (COA) that have a common goal and desired result. MDMP is an analytical technique that helps commanders and their staffs reach logical decisions in the employment of force. The military decision making process is fed information and products by several subsystems. Each subsystem is made up of staff estimates of the capabilities of their respective sections. The contribution is in the form of annexes and appendices to orders issued by higher headquarters. Input depends on the goal that MDMP is trying to accomplish. Information Warfare (IW) is the proponent of CNO. CNO is one of the core elements of IW. The mission is what dictates who will participate and their role in the process. If the mission is CNO, then all the other subsystems will support the proponent as necessary to ensure the success of the operation. If the mission is a more conventional mission then CNO is one of the subsystems that will support the overall operations. A hybrid of this is if the during a particular phase of the operation, CNO is the lead element, then the priorities change during that part of the execution. An assumption is that CNO will be used in support of an operation, the process is very similar, the difference being the priority of effort given

by supporting elements to the cause. In an unlimited time and space continuum, everyone receives all needed information and support. The reality is that main priorities are set and resources, such as time and personnel, are exhausted before everyone is satisfied. MDMP is a seven step process (Table 4) that begins with receipt of a mission in the form of an order to conduct an operation and ends with the Orders Production.

Military Decision Making Process	
Step 1	Receive the Mission
Step 2	Mission Analysis
Step 3	Course of Action Development
Step 4	Course of Action Analysis
Step 5	Course of Action Comparison
Step 6	Course of Action Approval
Step 7	Orders Production

Table 4. Military Decision Making Process

A commander then analyzes the order to determine how best to accomplish the original order's intent given the current situation. The staff will prepare multiple viable courses of actions to present to the commander. The commander decides on the best course of action and issues the order to execute or implement his decision. Computer network operations can be evaluated in using this format provided there is an established criterion to analyze. The lack of established criterion would make this process incomplete and, at best, a guessing game. Prior to step one, of MDMP, the staff must have estimates prepared as to their capabilities in relation to many contingency operations. In the CNO arena, the staff must know what is required to conduct a computer network attack or exploitation. The types of CNOs desired have a predetermined package or load out that includes the equipment (hardware), tools (software) and knowledge (personnel skills) to implement a planned operation successfully. The staff estimates would also include or list known vulnerabilities to different computer operating systems and the vectors that allow the operators take advantage of the weakness. These plans are generic and are a starting point to the planning process. Before conflict, CNO operators are planning operations and modifying or validating their staff estimates. These staff estimates include the intelligence preparation of the battlefield. The intelligence preparation of the battlefield attempts to

gain knowledge of the adversary and the targeted system. This includes how the adversary utilizes the targeted system. The primary goal of IO is "exploitation, corruption, disruption, degradation or destruction of [an] adversary information systems or their will to fight".[52] How CNO can cause or affect the enemies' ability to function is part of the staff estimate. The staff estimates are at best a 'game plan' without a specifically identified opposition. The opposition may be known, but the most current situation and desires (commander's intent) are not yet applied. When MDMP is initiated with an order from the higher headquarters, Warning Order or Operations Order, the planners apply the most relevant or applicable staff estimate(s) and begin the planning process.

Step 1	Receipt the Mission

The first step of MDMP is Receipt of the Mission. The Mission could be from the higher headquarters, such as the National Command Authority (NCA) or could be a progression from ongoing operations. The commander, after an initial assessment, provides guidance to his staff. This initial guidance is based on the commander's experience and his understanding of his staff's capabilities. The experience of the commander and his staff are based on knowledge or skills that have resulted from previous operations. Additionally, the group's synergy may dictate how much guidance the commander provides. The IO/CNO planning cell begins by reviewing the plan, identifying the mission and defining how CNO can assist in the overall operation. It is necessary to recognize whether the operation is primarily a CNO or a support element. This recognition has been the root of many conflicts among staffs and planning cells, and dictates who has priority. Every element or planning cell is important and all are dependant upon one another. The cell that is most important at particular junctions in the scheme of maneuver must be recognized so that resources, which are often limited, can be prioritized accordingly. For instance, an emergency medical evacuation (MEDEVAC) helicopter is crucial to any armed conflict or humanitarian mission. The resources

[52] *Joint Doctrine for Information Operations, Joint Publication 3-13*, 9 October 1998, p. I-9, [http://www.dtic.mil/doctrine/jel/new_pubs/jp3_13.pdf] September 2003.

expended on the survivability of troops may take higher priority over MEDEVAC in a combat environment. Given those same, competing resources in the context of a humanitarian mission such as Hurricane Andrew that struck Florida in August 1992, the MEDEVAC helicopter might take priority. It could be argued that survivability of the soldiers is always important, but depending on the current situation, threat, and mission, the priorities change. Upon receipt of the mission, the staff brings out its operational plans (define, plan with a general focus, but not specify date, times, or locations) and standard operating procedures to ensure the every element has a starting point to reference in MDMP, in preparation for step two. A key element is that the commander now dictates the allotted time for MDMP.

The responsibility of the IW/IO planning cell during step one is to have CNO staff estimates ready so that they may begin the process. The staff estimates are based on known intelligence about the enemy, their infrastructure, the order of battle, and how they use their information systems in support of the Enemy Course of Action (ECOA). The planning cell immediately evaluates the delta between the predetermined intelligence estimates and what is required by the task at hand. Actions must be planned to obtain the information from a higher headquarters, such as a Request for Information (RFI). An RFI is a formalized solicitation for necessary information through the higher headquarters or specific agency. The planners and organizational units must be prepared to conduct its own reconnoitering to gain the necessary intelligence of the battle space or Area of Operation (AO). Understanding of the AO is necessary to allow the staff to transition to the next step in MDMP.

Step 2	Mission Analysis

Analysis of the mission is where the initial intelligence is assessed. The second step of MDMP identifies the specific intelligence requirements to conduct an operation. The analysis determines what information and assets an organization possesses or has access to and identifies what is required to accomplish the mission. This information

leads to the development of a reconnaissance plan to gather the necessary information. The delta between information and assets available, and what is required is immediately identified. The delta of information is both requested and received or serves as a constraint to the planning process. Constraints are identified during this step and are imposed on the operations by Rules of Engagement, capabilities, organizational structure, area of operation (AO), and scheme of maneuver. In the most basic analysis of a CNO mission, the staff would determine if the mission is an attack or exploitation of a computer network. Important facts and assumptions are also identified and validated during this phase. The key element produced from this phase is the commander's intent. The commander's intent is a statement that defines success and the end state of the operation. The 'intent' is the guidance that must be incorporated in all the plans and courses of action that the staff produces. When the staff lacks specific instruction, the guidance serves as an azimuth or as the marker on the horizon for the staff to use as reference.

The entire staff dissects the directive and as group determines what is being ordered of the organization during step two. If there is any doubt or confusion, the commander requests clarification or resolution[53]. Specified and implied tasks are identified. The specified tasks are explicit, i.e., destroy the power grid at specified location no later than a specified date and time. Implied tasks are activities upon which the success of the specified task depends, e.g., conduct a reconnoiter mission of a specified power grid to determine targeting characteristics. During this step, the goal is to 'paint a picture of the battlefield, to provide the commander and the entire staff an understanding area of interest (AI) and the AO they are about to embark. The AI is the area with influence over the objective or organization plans which fall outside the boundaries established by the AO. For example, a homeowner's property is his AO, neighboring homes, roads, noise, parks, etc., that lie outside the homeowner's property line and impact his enjoyment, value, or use is his AI. In a combat operation, a unit's AO are the boundaries where it can normally dictate its own scheme or maneuver. The AI

[53] FM 34-8-2, Intelligence Officer's Handbook, May 1998, p. 3-2.

surrounding the AO may be of value in determining how the commander will maneuver his assets. During Operation Iraqi Freedom, Central Command's AO was Iraq. The sovereign country of Turkey and other countries that bordered Iraq were part of the AI, because they influenced the plans to conduct ground assaults into Iraq. Available assets are also determined during the analysis step. The staff determines what assets will fall under the organization's control the time period, and other resources necessary to accomplish the mission. The available resources may serve as a constraint to mission planning. Constraints to the operation are identified and listed for the entire staff. Constraints are organizational restrictions that prohibit certain actions, limit abilities or dictate an action. Time is a common constraint; it can limit the amount of planning; it can set boundaries during phased operations; and it can dictate an action by specifying when a target must be neutralized. Facts and assumptions critical to the mission planning are identified. Plans are made based on the facts and assumption of the higher headquarters, friendly and enemy situations, current battlefield conditions and intelligence. The facts and assumptions that impact the planning process or can influence the outcome of the operation are critical. This holistic approach to the analysis of the mission provides an understanding that assists all the planning cells in their preparation for step three of MDMP.

The role of the IW/IO planning cell is to identify the role of CNO within the operation. As specified and implied tasks are identified, the planning cell identifies what can be targeted using CNO to assist in the overall operation. The planning cell identifies each CNO target, why it is a CNO target, and the objective, based on the commander's intent. Network topologies for both the AI and AO are identified. If the network topology is accessible via WAN or LAN, AI and AO are relevant. The topologies provide possible entry points and vectors for CNA and CNE. The topologies include the links and nodes of the topology. If the specified or implied task is to reconnoiter, CNA can play a vital role. If the reconnoiter mission is to determine the level of enemy activity in preparation for battle, then a CNO task could be to identify the existence of traffic over a network, the amount of traffic, parties communicating, and message content. If the mission is to disable the power grid, then the role of non-kinetic energy

weapons can be called upon to target the SCADA system. The facts and assumptions identified by the CNO planning cell are the accessibility and vulnerability of the adversary's networks. If the adversary does not use computers, then CNA and CNE have little use in the operation. The constraints associated with the operation are also applicable to the CNO. If a unit is precluded from targeting a hospital, then a CNO operation with potential for negative, collateral effect on the hospital is an implied constraint. The constraints are identified and used in the process that the CNO planning cell can incorporate in a program. The capabilities of the use of CNO given the analysis are incorporated into step three of MDMP. The CNO cells divide, as do the rest of the planners, into separate groups to begin the Course of Action Development.

Step 3	Course of Action Development

The third step in MDMP is the development of Course of Action (COA). The goal of this step is to generate realistic options for the commander. The planners are separated into groups, each of which develops an independent COA. The CNO cell is divided and tasked to assist each group of planners in the development of plans. The COA must be viable; throw-away, trivial or impossible plans are not acceptable. The plans must be designed to succeed. Each COA is a distinct operation and is planned independently from the others. The number of troops and equipment is the same; how they are organized and arrayed may vary. The COA's suitability, feasibility, acceptability, distinguishability, and completeness must be identified. Suitability is the appropriateness of the unit's organizational structure to accomplish the mission. Feasibility is the practicability of the organization's ability to accomplish the mission. Acceptability is the tolerability or risk that the commander can tolerate for its action. Acceptability is not only defined by the commander; it is imposed by outside organizations, doctrines, Rules of Engagement, etc. Distinguishability is the clear difference between the other COAs, and is imposed by the commander. The commander may dictate part of the plan to differentiate between COA. In simple terms, he may dictate that COA I will be executed in daylight hours, while COA II is to be executed during cover of darkness. Otherwise, the plans may be similar. However, risk and

enemy's reactions may vary drastically. Each COA must be complete; and must be operationally comprehensive, from the designated starting point to the end state as defined in the commander's intent statement. The COAs clearly describe how the organization will fulfill the commander's intent. The number of COAs developed depends upon the size of the staff, time available to plan, and the size of the organization.

The role of the CNO planning cell is a significant part of the course of action development process. The CNO planning cell identifies the CNO target and assesses the capabilities of the organization, and the characteristics of the target. The cell develops the detailed plan on how it is going to accomplish its task and how the plan supports overall mission of the organization. Whether the task is CNE (alter or change or add and remove data) or CNA (deny, destroy, and degrade), the CNO planning cell is responsible for providing CNO capabilities to commanders and their staff.

A common technique is to follow a series of steps, identified in the book, Hacking Exposed, as Anatomy of an Attack (Figure 5). Anatomy of an Attack describes an attack methodology that involves identification of a network known as footprinting, a network executing the attack or exploitation, cleaning up, and creating and planting backdoors. Common steps for reconnoitering of a network or computer system are footprinting, scanning, and enumeration. The level of intrusiveness increases from the former to the latter. Footprinting is a systematic approach that enables the (operative) to create a complete profile of an organization's security posture[54]. It is electronic passive reconnaissance. The goal of footprinting is to discover information related to the organization's operational workspace without making direct contact with the target organization. Scanning is the active probing of a network to determine if the target organization is accessible through cyberspace. An example of scanning might be an active attempt to make contact with the target organization via the Internet or through email to determine if it is accessible by using certain network protocols. Enumerating

[54] McClure, S., Scambray, J. Kurtz, G. (2001). Hacking Exposed, 3rd Edition. Osborne/McGraw-Hill: New York, p. 4.

is the ability to glean information from the target organization by active probing from the discovery of the two previous steps, or if they failed to produce results. The key differences between the previous techniques lie in the levels of intrusiveness[55]. For example, to enumerate, an operative must be connected to the target organization. In a geographical sense, a border crossing to gather information is more intrusive compared to reconnaissance from the forward line of friendly troops (FLOT). Once the system is known and vulnerabilities are identified, the operators will attempt to access the system. Gaining Access occurs when enough data from the three previous steps has been obtained to make an informed attempt (at infiltration)[56]. Where enumeration is the act of obtaining passwords or keys, gaining access is their use to access the systems. With access to a system, escalation of privileges is attempted by either exploiting poorly configured systems or exploiting vulnerabilities. A poorly constructed system is a network that operates correctly, but is mis-configured from a security perspective. The exploitation of a vulnerability is the utilization of a system or program that was fundamentally flawed in its development. The former is a weakness in implementation while the latter exists in the development of software and devices. Both can be exploited to gain greater access and escalate privileges. The next step after entry is to escalate privileges. Computer systems are laden with permissions. Access is gained at one level of permission. Increasing the access privileges or permissions of an exploited user without authorization is known as "escalating privileges." Pilfering is further reconnaissance from inside the target organization's system. Pilfering evaluates trust among systems and identifies mechanisms to gain access to the other trusted systems[57]. With access and escalated privileges, the operator can commence the CNA or CNE. The next step, depending on the mission, is to cover up the intrusion. Covering Tracks is the elimination or hiding of evidence of the intrusion or attempted intrusion, from enumeration to pilfering. Modifying system logs or masking activity to appear normal and routine accomplishes this. A back door is an unauthorized entry point into a network system. Creating a Back Door is the act of leaving an avenue of approach that allows

[55] Ibid., p. 64.

[56] Ibid., Backcover.

[57] Ibid.

unauthorized access into the system by circumventing defenses and maintaining privileged access. These steps are not exclusive; a skilled operator may use a more unorthodox method, but in essence, the same goal is accomplished: successful attack and/or exploitation.

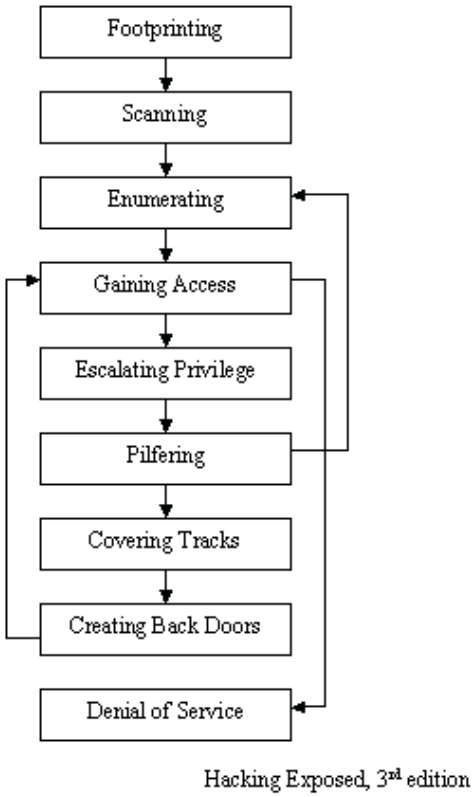


Figure 5. Attack Methodology

Targeting considerations are both quantitative and qualitative. During the COA development, the staff will produce measures or criteria upon which to base the viability of the plan or how close it compares to the commander's intent. The criteria will vary by individual operation. The criteria used for CNA consist of a combination of factors and characteristics identified in the CARVER and Schmitt analysis. The CARVER and Schmitt analysis has tools that help decision makers analyze and measure CNO targets. The former is more general in target analysis, while the latter provides a legalistic perspective to CNO. CARVER is comprised of several subcategories, each part defining

an aspect of the target and the necessary elements to determine the target's viability. The Schmitt analysis is a methodology for measured response to computer network operations developed Michael N. Schmitt, professor of International Law, at the George C. Marshall European Center for Security studies.

MDMP is fed by information; part of that information is target analysis. CARVER is a methodology used for target analysis and vulnerability assessment by special operations forces (SOF). CARVER is an acronym for Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability. Each element defines an aspect of a target and the necessary facts to determine its feasibility to engage. CARVER attempts to simplify target descriptions into manageable elements. Each element has a distinct objective to prevent overlap of criteria and provides the decision maker clear and concise information. This information is used by mission planners to decide whether a target will be engaged, and to shed insight as to how best to engage the target. The CARVER methodology's measurable factors are described as follows:

- Criticality. Criticality, or target value, is the primary consideration in targeting. A target is critical when its destruction or damage would significantly impair an enemy's political, economic, or military operations. It may also be critical to observe a target in a special reconnaissance (SR) mission (e.g., a key road junction for signs of major enemy movement). Individual targets within a target system must be considered in relation to other elements of that system. The value of a target may change as the situation develops, requiring the use of time-sensitive targeting methods.
- Accessibility. In order to damage, destroy, or conduct surveillance of a target, SOF must be able to reach it, either physically or via indirect (i.e., standoff weapons or surveillance) means. During SR missions, SOF must not only be able to reach the target, but must often remain there for an extended time period. Finally, SOF must be able to exfiltrate out of the target area.
- Recuperability. In the case of direct action (DA) missions, it is important to estimate how long it will take the enemy to repair, replace, or bypass the damage inflicted on the target. Recuperability is a vital supporting element of criticality. A target may not be lucrative for SOF employment if it can be repaired, replaced, or bypassed in a short time with minimum resources.

- Vulnerability. A target is vulnerable if SOF has the means and expertise to conduct the planned mission and to achieve the desired level of damage or other objectives as assigned.
- Effect. For targets of a more purely military value (e.g., munitions depots; headquarters complexes; Petroleum Oil and Lubricants (POL) facilities; Lines of Communication (LOCs); and Command, Control, and Communications (C3) complexes), the impact of both attacking (or surveilling) the target and achieving the desired results must be assessed. For targets that are critical in both the military and civilian regimes, the political, economic, legal, and psychological effects of the mission must be evaluated as well as the impact of target destruction on the health and welfare of the indigenous civilian population.
- Recognizability. The target must be identifiable under various weather, light, and seasonal conditions and configurations (if applicable) without being confused with other targets or target components. Sufficient data must be available for SOF to differentiate the target from similar objects in the target area. The same requirement exists to distinguish the target's critical damage points and stress points from their parent structures and surroundings.[58]

The six aforementioned factors provide both decision maker and operators an idea of the complexity of the mission and the ability to engage the target effectively.

The Schmitt methodology identifies six categories for use in analyzing CNO[59]. Additionally, this methodology adds a quantitative weight to each category. These categories correspond directly to attributes associated with computer networks and the resulting consequences if and when targeted. The six factors that the Schmitt Analysis describes are severity, immediacy, directness, invasiveness, measurability, and presumptive legitimacy. Additionally, the categories are weighted to reflect the degree of consequence for each factor. Schmitt defines the six criteria from a legalistic approach.

The severity factor measures the physical damage or harm inflicted as a result of targeting a system. The destruction or harm is equivalent to the battle damage that results

[58] Joint Special Operations Targeting and Mission Planning Procedures, 10 August 1993, p. II-9, [http://www.adtdl.army.mil/cgi-bin/atdl.dll/jt/3-05.5/jp3_05_5.pdf] September 2003.

[59] Schmitt Computer network Attack and The Use of Force in International Law: Thoughts on a Normative Framework, June 1999, p. 18.

from kinetic energy. Bomb damage assessment (BDA) identifies the effect of kinetic munitions. Schmitt uses severity to describe "armed attacks (that) threaten(s) physical injury or destruction of property"[60]. It is an attack on the "physical well-being (usually occupied by) the apex of the human hierarchy of need"[61]. Severity identifies the kinetic resultant of the attack.

Immediacy is the factor that applies time and spacing in relation to the effect of the attack. The timing is relevant to the operation. During an air attack, a CNA directed at the suppression of air defenses, seconds are critical compared to an economic embargo where the target is to deny the opposition use of an information-specific system.

> The negative consequences of armed coercion, or threat thereof, usually occur with great immediacy, while those of other forms of coercion develop more slowly. Thus, the opportunity for the target state or the international community to seek peaceful accommodation is hampered in the former case[62].

By the nature of each operation, timing is relative to mission objectives and period allocated for the implementation.

The directness factor is the desired impact of the operation that can be specifically traced to resultant effects of a CNO. The number of combat systems added to an operation increases the number of variables and dilutes the directness of any one system. Directness precisely links an action to a reaction.

> The consequences of armed coercion are more directly tied to the actus reus than in other forms of coercion, which often depend on numerous contributory factors to operate. Thus, the prohibition on force precludes negative consequences with greater certainty[63].

---

[60] Ibid.

[61] Ibid.

[62] Ibid.

[63] Ibid.

The ability to identify consequences and directness allows commanders to gauge the operational response with a known outcome. The directness of the effect can determine whether the CNO is the main operation or is in support of an operation, depending on the acceptable levels of hostilities.

The level of infringement upon the rights or property of the target is addressed by the invasiveness factor.

> In armed coercion, the act causing the harm usually crosses into the target state, whereas in economic warfare the acts generally occur beyond the target's borders. As a result, even though armed and economic acts may have roughly similar consequences, the former represents a greater intrusion on the rights of the target state and, therefore, is more likely to disrupt international stability[64].

In a fist fight, levels of invasiveness can be compared to a punch in the mouth and an errant swing that misses the target. Both acts are invasive to one on the receiving end of the fist. Their levels of invasiveness however, are quite different in terms of effectiveness. In terms of certain penal codes, the wild swing is assault while the connecting punch is also classified as battery. In a nautical comparison of invasiveness, a warning shot across a ship's bow is less grave then a direct hit.

The factor of measurability addresses the consequences attributed to the CNO. An action that results in equivalent kinetic energy damage can be measured. Collateral damage is measured as is the probability of its occurrence. The collateral damage must be considered because inflicting such consequential damage may exceed the acceptable risk or scope of the operation.

> While the consequences of armed coercion are usually easy to ascertain (e.g., a certain level of destruction), the actual negative consequences of other forms of coercion are harder to measure. This fact renders the appropriateness of community condemnation, and the degree of vehemence contained therein, less suspect in the case of armed force[65].

---

64 Ibid.

65 Ibid.

An action resulting in a system's latency over a long period of time will be less obvious. The measurability factor attempts to determine all consequences of the actions taken.

Presumptive legitimacy deals with the laws, customs, treaties, binding agreements, and Rules of Engagement associated with the operation. It is the legality and authority of the operation, measured by various standards and recognized authority to conduct the operation.

> In most cases, whether under domestic or international law, the application of violence is deemed illegitimate absent some specific exception such as self-defense. The cognitive approach is prohibitory. By contrast, most other forms of coercion—again in the domestic and international sphere--are presumptively lawful, absent a prohibition to the contrary. The cognitive approach is permissive. Thus, the consequences of armed coercion are presumptively impermissible, whereas those of other coercive acts are not (as a very generalized rule).[66]

The conventional forces of DoD do not have the flexibility to decide at the operational level on the presumption of law. This presumption is likely to be identified in advance. The goal of the operator is to determine the scope of the presumptive legitimacy.

The factors identified have an associated, logarithmic scale that applies a weight or value to each. This weight provides a quantitative measure to the analysis. The scale can vary so long as it is consistent in terms of what it is measuring and is applied consistently to achieve and assess the correct metrics.

Step 4	Course of Action Analysis

Analysis of the COA, step four, is also described as war gaming. It tests each COA against the criteria discussed in step three of COA development, and includes other

[66] Ibid.

conditions cited by the commander. This step does not compare one COA to another. The analysis must be unbiased, and must not be designed to favor one COA over another. War gaming the plan identifies advantages and disadvantages of each individual COA. War gaming tests the flow of the operation and how the organization will act, react and how it will counteract actions and events identified by the COA and threat expectations Each plan must be evaluated against many possible outcomes, based on the situation and known variables, such as enemy disposition. At a minimum, the worst-case scenario and the most likely or probable action by the enemy should be used to test each COA. Time will dictate how many scenarios are likely to be tested. The final step of war gaming is to modify the COA to ensure both that it can be implemented and that it satisfies the commander's intent.

It is the CNO cell's responsibility to provide the operation with means and methods to target the enemy's Centers of Gravity (CoG). The CoG are those characteristics, capabilities, or sources of power from which a military force derives its freedom of action, physical strength, or will to fight[67]. The CoG uses information to operate effectively. It is the responsibility of the cell to identify the links and nodes of the network that is passing and storing the information. When the network topology is identified, then vulnerabilities are analyzed. Once the targets are identified, they are measured against the established criteria. The CNO cell cannot plan this action in a vacuum. The intelligence cell (J2/N2/G2) provides the enemy's actions and reactions[68] during the war gaming process. The J2 provides an intelligence estimate of what to expect from the enemy based on doctrine, tactics, lessons learned and any other of the myriad intelligence inputs. The CNO plan provides details of how it can influence or use a Named Area of Interest (NAI) to assist in intelligence gathering. An NAI is the geographical area or object with information that will satisfy specific requirements. The information collected within the NAI will help to confirm or deny a particular enemy course of action.

---

67 [http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-06/gloss.pdf] March 2004.

68 FM 34-8-2, Intelligence Officer's Handbook, May 1998, p. 3-4.

A situational template portrays how a CNO will influence the battle space given this COA. The template mirrors the phases of the overall operation, and identifies the targets and plan of engagement for each. The targeted systems must be important to the operation and must synchronize with the overall scheme of maneuver. The CNO plan must be honest about capabilities and expectations, and is based on facts and assumptions that support the operation's outcome. The facts and assumptions are validated by the J2 and the entire planning staff. Once a comprehensive plan is completed, it is submitted for comparison to the other COA.

Step 5	Course of Action Comparison

The comparison of COA to one another occurs during step five, the goal being to identify the best COA. The planning staff reconsolidates and objectively evaluates each COA. Each planning staff presents their COA, the objective is to identify the best COA, not sell the plan. The commander and staff members must be aware that ownership to a plan may develop. Ownership reflects the desire for one's plan to outperform other COA. This desire can impact the objective presentation and analysis of the COA. COA are objectively assessed using quantified and qualified measures rather than presentation skills. The criteria are weighted to add value based on the commander's guidance. The commander will use the weighted variables based on their decisiveness in the overall operation. All COAs will be judged on the same criteria. The best COA is defined by the highest probability of success based on the criteria established by the commander. The COA can be tracked in the phases of the operation. The phased approach allows for adjustment of the evaluation criteria's importance as focus of the battle changes. For instance, a criterion may be to maintain the element of surprise during the operation. During phase one of the operation, the element of surprise may be weighted to reflect its importance, where that same criterion may not be as relevant during subsequent operational phases. The comparison of COAs and the evaluation criteria allow the commander to compare different concepts of the same operation with one standard grading mechanism.

During step five, the CNO cell consolidates and provides an objective evaluation of the CNO portion of all COA. The CNO cell validates the intelligence necessary to execute all proposed plans successfully. Each plan is then given a score, based on the criteria. The commander expects and depends on the CNO's cell technical competency to validate this portion of the operation. Once all of the COAs are compared, the commander decides on the most effective COA. This assessment is based on quantitative and qualitative measure.

Step 6	Course of Action Approval

The commander's decision is the sixth step of MDMP. This step is the approval or modification of a single COA, a modification of all COAs, or a more narrow focus of one COA that contains attributes of other COAs. The commander's decision may require that the war gaming process, (step 4 of MDMP), recommence based on new guidance provided by the commander. If the commander does reject a COA, modifications may be required. In event of such rejection, the commander must provide guidance and the staff must return to step 2, Mission Analysis. When the commander approves a single COA at the end of this process then the planning phase is complete.

Step 7	Orders Production

The final step of the MPMP is production of the order. The order, or Operations Order (OPORD), is distributed to subordinate commanders so that they may plan and execute the stated objectives of the higher headquarters. The OPORD contains the scheme of maneuvers dictating how the commander expects to fight the battle. The scheme of maneuver - the part of the order that directs the sequence of battle - directly reflects the COA that the commander decided to implement during the previous six steps of the MDMP.

2. New CNO Methodology Resultant Equities

The Computer Network Operations methodology proposes that you can inject extrapolated data from the CARVER targeting methodology and the Schmitt analysis into the military decision-making process. The data to be incorporated must be clearly defined in order that it can be used uniformly across different commands and by different decision makers. The factors identified in CARVER and Schmitt can be combined to determine a single and more complete listing of factors that will be utilized in evaluating the proposed applications of CNO. The combined factors can either be used exhaustively in the decision process or they can be utilized in a modified form that accelerates the decision making process. The factors are defined in an operational sense to describe their applicability to operators. The explanations of the factors are presented to allow one common definition and criterion for evaluation and comparison. By having clear and concise definitions, commanders can have common principles to evaluate across multiple platforms.

Criticality- Criticality defines the importance of the target in relation to the overall mission. Criticality is defined as "a system or asset that, if attacked, would result in catastrophic loss of life and/or catastrophic economic loss"[69]. From a military perspective, the criticality of a system is determined by its importance to the success of the operation. Criticality is clouded by targets that serve dual use, in both the civilian and the military infrastructure.

Accessibility- The ability to reach the targeted system, accessibility can be measured in various ways. Ease of access to exfiltrate must also be considered. Questions that need to be addressed are Is the target reachable from outside the network via the WAN or must the target be accessed from within the LAN? Can the operator and the data be removed or exfiltrated?

---

[69] California Office of Homeland Security (OHS), FY03 State Homeland Security Grant Program, Part II [http://www.oes.ca.gov/Operational/OESHome.nsf/PDF/CIPinstructionsFinalpdf/$file/CIPinstructs.pdf] February 2004.

Three categories that can be addressed are delivery vectors, payload insertion and the entry points to the network. For instance, can the payload can be injected from the WAN using a vector? Must the payload be inserted from within the LAN without an allied operator (e.g., as an e-mail attachment)? Must the insertion be performed from within the LAN by an operator (requires no monitoring, requires the operator to execute code and/or harvest information)?

Recuperability- Recuperability is the ability for the target system to regenerate the processes or to work around the problem. This is time-critical in relation to the operation. The assumption is that, given unlimited time, all targets are recoverable or the effect can be mitigated. The ability for the enemy to bypass or breach an obstacle is relative to the sequenced timing of the mission's execution.

Vulnerability- Do the operators have the means and knowledge to execute the mission? How complex is the mission, including infiltration and exfiltration of operators, and the level of technical expertise and knowledge of the targeted system? Means, knowledge and technical expertise vary drastically, depending on which team conducts the mission. Expertise in one technical field does not necessarily carryover to other technical fields. This must be assessed based on the team's technical and tactical abilities.

Effect- While it is the desired consequence of the action, effect considers the action's worst possible collateral consequence and the probability of its coming to bear. Probability of the most likely outcome of the action is taken into account. A weapon's effectiveness is key to determining its direct effect.

Indirect effect requires more planning and thought, and may vary depending on the geopolitical culture of the target and the intended audience. The difficulties in measuring the indirect effect are exemplified by comparing the reaction of two computer

terminal operators when the system is latent. One operator may be flustered, impacting his ability to focus and perform, while the other turns his attention to non-network duties without frustration. Predicting the outcome requires, not only the knowledge of the system, but understanding the enemy that is working on the target systems. The effect can be as much physical as psychological, and must be explored to ensure that the difference between the desired effect and the actual result are within the acceptable risk of the decision maker.

Recognizability- It is essential to be able to identify the targeted system within a maze of cyberspace. One cannot target what he cannot identify. Recognizability includes an understanding of the topology interconnecting the targeted system as well as the scheme's redundancies. Depending on the operation, the need to pinpoint the system may not be as necessary. This is true if the system can be neutralized by targeting a single point of failure in the network topology, where attack on that point would accomplish the mission. The bigger the footprint of the attack, the more likely one will reach the intended target.

Severity- In terms of brutality and audaciousness, severity is different from effect. While severity measures the amount of physical destruction or harm that can result from the attack, Effect measures the likelihood of achieving the end result.

Severity is situation-relative. In attempting to create traffic congestion, consider the following possibilities. Disabling a traffic signal in a rural community does not compare to disabling the tollbooth traffic signals on San Francisco's Golden Gate Bridge at the beginning of rush hour traffic. Couple that with a system that is used to save lives. By targeting the emergency management system (911) that controls police, fire, and other emergency first responders, the severity of an emergency can be aggravated to increase the number of casualties.

Immediacy- The interval between successful execution of the operation, viewing battle damage, and achieving the desired effects is known as immediacy. When the commander wants to see the desired effect is the key point to immediacy. Does an operation's success, require instantaneous results or will a gradual reaction, over an extended period of time, suffice? When considering immediacy, the reaction of the target and its ability to counter the action must also be well thought-out: for instance, an instantaneous action that can be quickly countered, thus negating the action. A target's ability to counter CNO successfully can be attributed to the time available. Immediacy can also be determined by time and space. Is the target fleeting, thus offering a limited or short engagement availability? Is the target one of opportunity, that can be easily engaged once positively identified?

Directness- Directness is the ability to determine the cause of the severity and its effect, and to associate that with the CNO operation. Consider engaging a target with one weapon system, such as a sniper, and effectively immobilizing a military leader vs. a combined arms attack that includes ground, air and naval forces that targets that same military leader. Who caused the immobilization can be difficult to ascertain. In CNO, directness may be necessary to measure the usefulness of the tool.

Invasiveness- The level of intrusion defines the level of invasiveness. To conduct surveillance from the friendly or neutral side of a border, or by using highly technical equipment that can be commanded from afar, is less invasive then inserting someone into a sovereign entity to load a tool or exploit that will enable the surveillance. The current state of hostilities between the combatants influences the level of invasiveness permitted.

Measurability- The ability to quantify the effect in degrees of physical destruction, economic damage, magnitude or causing someone to act or not act based on the CNO is the measurability factor. Measurement can be done in quantity, (i.e. the

number of troops killed or number of buildings destroyed) or in terms of absolute comparison (i.e., more than, less than, or equal to). A binary measurement tool can also be used to determine an action or inaction: true or false, yes or no, on or off. The quantifier should be applied in a manner that provides meaning to the decision maker.

Presumptive Legitimacy- The assumption that the action is just and defendable by not only laws or customs, but by less precise measures such as ethics and codes of conduct. At a military operational level, the laws of war apply as well as individual ethics. Proportionality is one of the aspects of Presumptive Legitimacy; different from Effect and Severity, it deals with a response to an action. Presumptive Legitimacy is tied to geopolitical factors and how they are applied to hostilities or level of hostilities in general.

An appropriate metric is needed to allow commanders to visualize the results of their decisions. A template can assist in evaluating the acceptable level of risk or exposure (Figure 6). The proposed CNO Resultant Equities Model (REM) provides control that a commander can use to align his warfare knowledge with the capabilities of CNO as a weapons system. The REM organizes factors into evaluation criteria. The evaluation criteria are presented in the form of a question to the COA developers. This question is derived by integrating the CNO factors and the commander's intent, applicable ROE and other applicable limitations and constraints. The question or query is the Issue in Question (IQ) in the CNO RE Model. With the IQ identified, a Unit of Measure (UM) is developed. The UM can be quantitative, qualitative, binary or benchmarked, as long as it can be logically justified and is appropriate to what the commander is attempting to compare. The UM is given a rating on a scale. The scale is consistent throughout the REM, it can be 1 to 10, with 10 being optimal or 10 to 1, 1 being optimal, as long as the desired result is consistent

The desired result defines the scale; the staff is either pursuing a high or low score depending on IQ and UM. The REM further brackets possible outcomes from a best-case to a worst-case scenario. The brackets do not have to be uniform in size. The principle measure of bracket size is each bracket's ability to distinguish cut off points. In a monetary evaluation, an amount of money might be the distinguishing factor, e.g., "> $1,000" or "< $1,000". In a budgeting application, that same monetary measure may not apply; a better cut off might be measured by reimbursable, funded, or unfunded requirement. Both examples address monies, but in context, they have different meanings to the decision maker. The brackets are aligned with UM as depicted in the severity example.

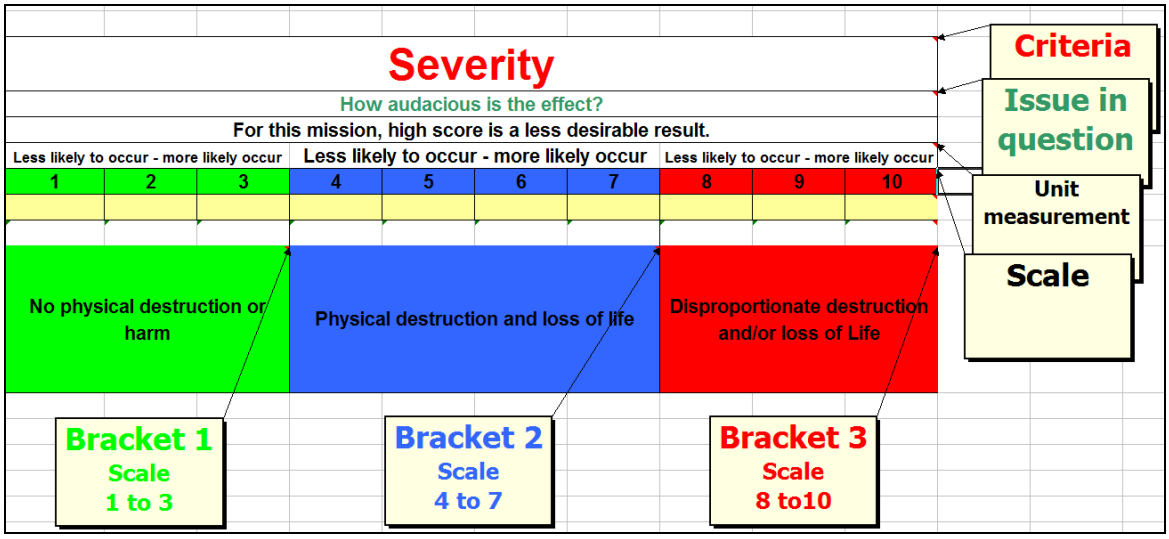


Figure 6. Severity

The commander and the planning staff determine the factors to be used for COA evaluation. The REM is used to compare the COA during step 5 of MDMP. The IQ, UM, scale and brackets are tailored to the operation. The REM is created to determine the best COA, not make one COA more attractive or palatable then another. During the COA comparison, when the IQ is addressed, the worst-case outcome is selected by assigning a 1 to the box below the appropriate and expected outcomes. Assigning the 1 activates a formula that will output a number known as the Resultant Equity (RE). RE is a quantified measure of risk for the given input. The REM will only recognize the worse

or highest value. The commander can add importance to scale by applying weight to the factors (Figure 7). Most often, weighting factors are multipliers. Make sure that weighting is correct and meets the commander's objectives. The weight multiple is added to the RE, increasing its numerical value when greater then 1, and reducing its value when less then 1. Additionally, the commander can set a benchmark to identify a value that warrants scrutiny if it is exceeded. This is known as the Resultant Equities Threshold (RET). In the example below, the weighed criteria has a multiple of 2 and a RET of 15. The output is multiplied by the value of the weight. A value of 15 will result in an output of DANGER next to the RE.

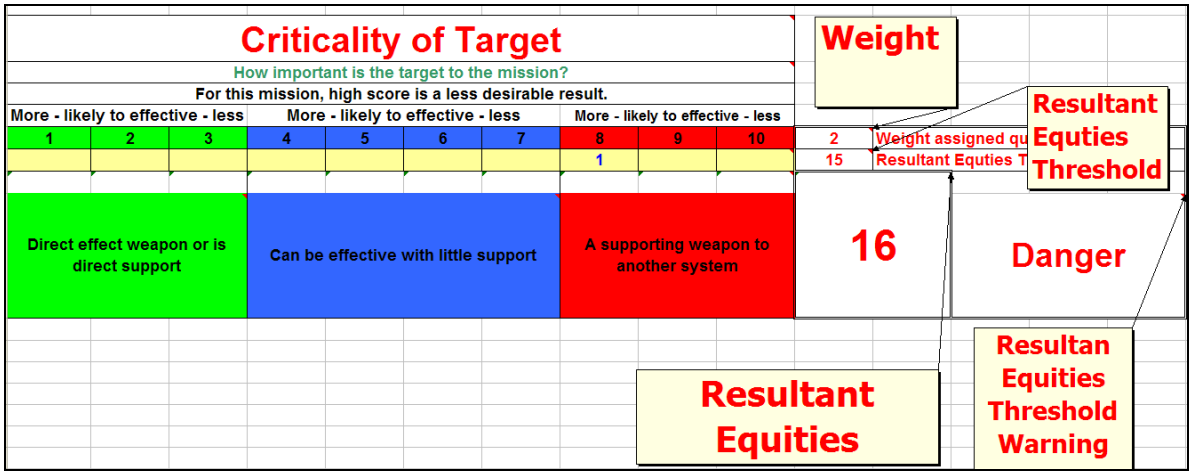


Figure 7. Criticality of Target

The formula for this output is [(expected worse case scenario Unit of Measure) multiplied by selection] multiplied by weight] = resultant equities. If resultant equities exceeds 15, "Danger" is displayed. Mathematically, [(8)*1]*2=16; if 16 > 15, then Danger. Weighing these factors must be consistent with other valuation schemes currently being used by decision makers to assist in assessment of proposed plans.

The REM is used with other methodologies to assist the commander in decision making. The methodologies allow the commander to compare different aspects of a CNO and to quantify the output. The goal of the CNO is to frame and populate the formula accurately in order to obtain a quality output. CARVER and Schmitt provide a

foundation for the criteria and issues in question. The CNO cell has the responsibility to address all factors in context of the operation. The commander and staff have responsibility to understand what is necessary to conduct CNO. This understanding allows the accurate COA analysis and comparison. MDMP, CARVER, Schmitt and REM serve as a decision support system for the commander and staff. Used correctly, it can enhance the success of an operation. Used incorrectly it can be useless, or in a worst-case scenario, can cause the organization to pursue a COA that is fundamentally flawed thus wasting resources.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. FINDINGS AND RECOMMENDATIONS FOR FURTHER RESEARCH

There is a capabilities gap between the emerging and future threats and commanders' ability to attack and exploit the battle space. The President has already emphasized the need for a strategy to address this gap. It is now up to DoD to conduct a thorough analysis and to identify current capabilities and integration into the armed forces. The Joint Capabilities Integration and Development System (JCIDS) (Figure 8) is an appropriate model to conduct the analysis. CNO can be developed as a traditional weapons system. Beginning with a review of the doctrine how we fight and win our nations wars. By using JCIDS many of the questions that arise from this emerging technology can be addressed with the right Joint focus. The Functional Area Analysis (FAA) will provide the task, conditions and standards for the employment of CNO. The Functional Needs Analysis (FNA) assesses the capabilities gap between current and future objectives. The capabilities gap can be bridged using the Functional Solutions Analysis (FSA). The FSA is a review of the core components of the military, and includes: Doctrine, Organizational, Training, Material, Leadership/Education, Personnel, and Facilities (DOTMLPF).

During FSA, the evaluation of DOTMLPF and how a change to one or more of the components can contribute to bridging the capabilities gap. Each proposed change is identified, analyzed, and alternatives are evaluated and compared to other alternatives. The output of the analysis is the recommended change to the existing DOTMPLF. These changes are reviewed by Post Independent Analysis (PIA). The PIA is an independent review board that evaluates not only the recommended changes, but the process that was used, facts and assumptions, and any other relevant variables to determine the best changes to integrate into DoD. Inputs to this process are the Initial Capabilities Document (ICD), Capabilities Development Document (CDD) and the Capabilities Production Document (CPD). These documents identify the capabilities gap, evaluation of DOTMLPF, current technology available, ability to develop new technology, and

whether capability exists to produce the weapons system given the current and potential technology. The following example illustrates the process, with evaluation focus on the Materials portion of the DOTMLPF.

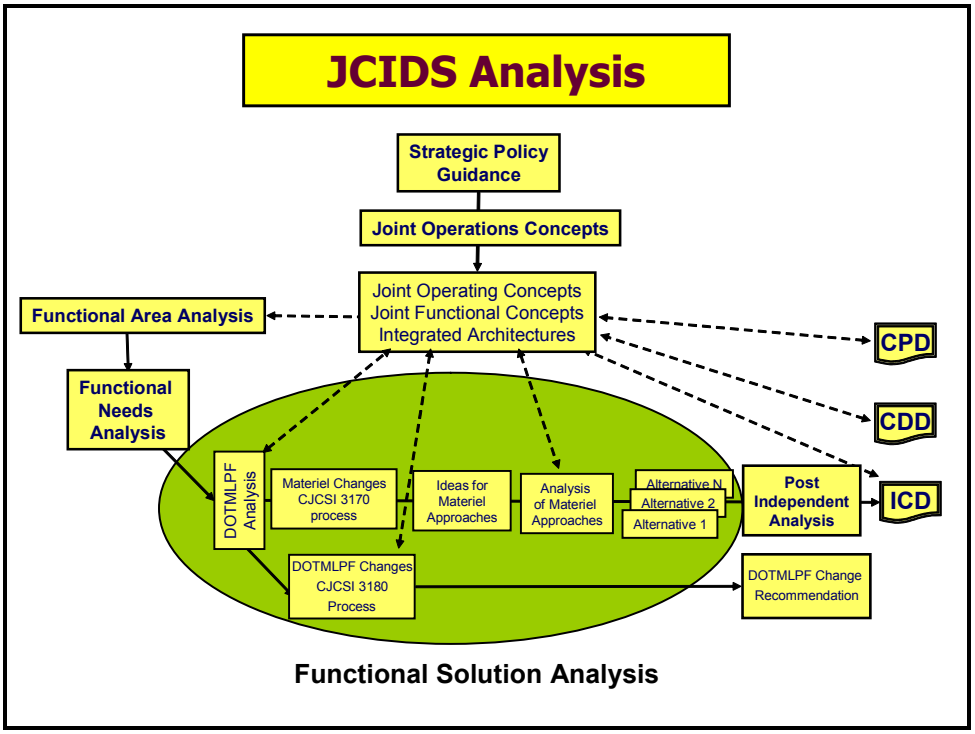


Figure 8. JCIDS Analysis[70]

Here are some of the obvious questions that can be addressed in relation to CNO and DOTMLPF:

- **Doctrine** - How can CNO be incorporated in doctrine at the Joint and Component level?
- **Organizational** - How should units organize to utilize CNO effectively?
- **Training** - How do we train operators to conduct CNO?
- **Materials** – What materials or tools do we have to conduct CNO and how do we use them?
- **Leadership and Education** – How do we inform commanders regarding the use of CNO as a weapons system?

[70] Tudor, Rod, LTC, Naval Postgraduate School, January 2004.

- **Personnel** – How do we recruit skilled, technical operators that are in high demand due to their transferable skills in the civilian market place? Can this need be outsourced to civilian contractors? Can conventional operators be trained to conduct these missions?
- **Facilities** – What facilities are necessary to train and sustain the CNO mission.

There are two types of information operation: offensive and defensive. "Offensive operations involve the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence"[71]. This research focused on the offensive nature of CNO. Further research is required to develop a defensive capability for US cyber infrastructure. "Defensive operations integrate and coordinate policies and procedures, operations, personnel, and technology to protect and defend information and information systems"[72]. US adversaries have much more to gain from CNO than does the United States. Action must be taken to harness this new weapon and harden our systems. The US ability to get into the battle space of their opponent is unprecedented; however, this over reliance on technology can be a hindrance as well.

[71] The Information Warfare Site [http://www.iwar.org.uk/iwar/] September 2003.

[72] Ibid.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. CONCLUSION

Computer Network Operations have the potential of great impact, either as offensive or defensive weapons. This duality of purpose makes CNO difficult to counter. A more complex network topology increases risk of penetration and exploitation. When a commander has greater understanding of the network components, he is better suited to make informed decisions on precise targeting.

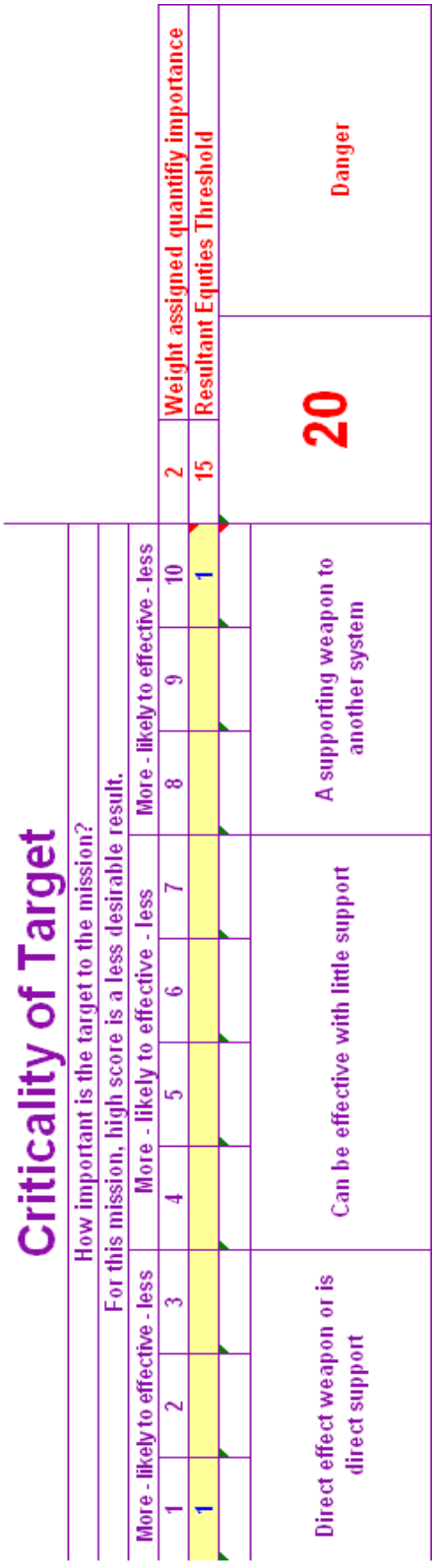
The proposed methodology provides a qualitative and quantitative means to address CNO. The methodology cannot stand alone. To be effective it must be infused with accurate and pertinent intelligence. This intelligence focus should contain traditional elements such as composition of enemy forces, but it should also include CARVER and the Schmitt analysis. By understanding what to look for in CNO intelligence, commanders will know what to analyze when contemplating COA and potential objectives.

To what extent should the Department of Defense utilize the new technology? It is important know the capabilities and limits of the weapons. How does the US reign in the power when potentially anyone with a rudimentary education, the ability to read, and access to the internet can be a viable player in the battle space of CNO? The US military has educated and informed personnel and provides the tools that have a dual use for normal functions and CNO in the form of computers, networks and connectivity beyond the local area network. The combination of personnel and the platforms for CNO warrants the control of this weapon system. Military leaders have strict supervision and controls of conventional weapons, such as pistols and the ammunition, yet do not necessarily view their own networks as potential weapon systems that can be decisive in battle. Those who do, may not have the scope to exercise the potential of CNO efficiently or effectively without the necessary command and controls functions in place prior to engagements. In one aspect, a commander may use CNO as a weapon to cause a desired effect, it is the undesired 2nd and 3rd order effects that may be less desirable that

he may not be able to control or assess like conventional weapons. The weapons and platforms for CNO are readily available, so strict controls must be implemented to ensure the decision maker(s), who has the appropriate responsibility and accountability, is in command of this power.

The United States is more susceptible to an effective CNO attack and reprisal due to its military's growing dependence on computers and networks. Susceptibility to counterattack is so great that computers' use must be contemplated while measured against DoD's ability to be prepared for war. The end state should be for DoD to be at the apex of readiness while realizing the geopolitical nature of warfighting and the norms, opinions and attitudes of world community. There are two counterpoints to CNO. Just because it can, does not give the US the mandate to conduct CNO and the counter argument is because the US can, it should. The decision to act or not act should exercise command and control, such as the proposed methodology, for commanders to make informed decisions and act responsibly when preparing for operations.

APPENDIX. TARGET INFORMATION



Criticality of Infrastructure

What is the likely hood of impacting the Critical Infrastructure?

For this mission, high score is a less desirable result.

Less likely to occur - more likely occur			Less likely to occur - more likely occur				Less likely to occur - more likely occur				
1	2	3	4	5	6	7	8	9	10	3	Weight assigned quantifiy importance
			1							15	Resultant Equties Threshold

Pure military infrastructure	Dual use Infrastructure	Civilian Infrastructure	12	

Criticality of Target in relation to Time

How much time is required to from target identification to engagement?

For this mission, high score is a less desirable result.

Less - time- More			Less - time- More				Less - time- More		
1	2	3	4	5	6	7	8	9	10
							1		

1	Weight assigned quantifiy importance
15	Resultant Equties Threshold

Target of Opportunity*	Sufficient planning time is available given a precise target	Fleeting*	8

Accessibility

Given the assets available, is the target accessible?

For this mission, high score is a less desirable result.

More likely - Access - Less likely			More likely - Access - Less likely				More likely - Access - Less likely				
1	2	3	4	5	6	7	8	9	10	2	Weight assigned quantifiy importance
									1	15	Resultant Equties Threshold
Accessible via WAN from allied platform			Can be executed from within the LAN without human intervention (i.e. .exe file)				Accessible from direct human intervention from within the LAN			20	Danger

Accessibility for exfiltration of troops

What is the likely hood of extracting personnel from the target?

For this mission, high score is a less desirable result.

Less - time- More			Less - time- More				Less - time- More		
1	2	3	4	5	6	7	8	9	10
		1							

3	Weight assigned quantifiy importance
15	Resultant Equties Threshold

Target of Opportunity*	Sufficient planning time is available given a precise target	Fleeting*

9

Accessibility for data extraction

What is the likely hood of extracting data from the target?

For this mission, high score is a less desirable result.

More likely - Access - Less likely			More likely - Access - Less likely				More likely - Access - Less likely		
1	2	3	4	5	6	7	8	9	10
					1				

1	Weight assigned quantifiy importance
15	Resultant Equties Threshold

Accessible via WAN from allied platform	Can be executed from within the LAN without human intervention (i.e. .exe file)	Accessible from direct human intervention from within the LAN

6

Recuperability

For this mission, high score is a less desirable result.

For this mission, high score is a less desirable result.

Less - time- More				Less - time- More				Less - time- More			
1	2	3	4	5	6	7	8	9	10	2	Weight assigned quantifiy importance
				1						15	Resultant Equties Threshold
No capability			Somewhat capable				Very capable			10	

Recuperability - bypass

Does the system(s) have the capability to bypass attack through redundant systems?

For this mission, high score is a less desirable result.

Less - time- More										Less - time- More
1	2	3	4	5	6	7	8	9	10	
	1									
No capability		Somewhat capable					Very capable			

3	Weight assigned quantifiy importance
15	Resultant Equties Threshold
6	

Vulnerability

Does the capability exist to exploit or attack the target?

For this mission, high score is a less desirable result.

High - Probability - Low							High - Probability - Low		
1	2	3	4	5	6	7	8	9	10
					1				

1	Weight assigned quantifiy importance
15	Resultant Equties Threshold

System can be attacked using normal operating procedures.	Vulnerability and exploit on hand	Exploit does not exist – not vulnerable

6

Effect – based on probable enemy COA

Can we achieve the desired effect given the probable or likely enemy reaction to the COA?

For this mission, high score is a less desirable result.

High - Probability - Low			High - Probability - Low				High - Probability - Low		
1	2	3	4	5	6	7	8	9	10
							1		

2	Weight assigned quantifiy importance
15	Resultant Equties Threshold

Direct and Indirect effects calculable	Direct or Indirect effects calculable	Direct and Indirect effects incalculable	16	Danger

Effect – based on enemy worse case scenario COA

Can we achieve the desired effect given the worse case scenario enemy reaction to the COA?

For this mission, high score is a less desirable result.

High - Probability - Low			High - Probability - Low				High - Probability - Low		
1	2	3	4	5	6	7	8	9	10
			1						

1	Weight assigned quantifiy importance
15	Resultant Equties Threshold

Recognizability	Direct or Indirect effects calculable	Direct and Indirect effects incalculable	4	

Recognizability

Can the target be identified?

For this mission, high score is a less desirable result.

High - Probability - Low							High - Probability - Low							High - Probability - Low			
1	2	3	4	5	6	7	8	9	10		3	Weight assigned quantifiy importance					
1											15	Resultant Equties Threshold					
Use of indirect means can pin point target			Combination of direct and Indirect means can pin point target				Use of direct means can pin point target				3						

Severity

How audacious is the effect?

For this mission, high score is a less desirable result.

Less likely to occur - more likely occur			Less likely to occur - more likely occur				Less likely to occur - more likely occur		
1	2	3	4	5	6	7	8	9	10
		1							
No physical destruction or harm			Physical destruction and loss of life				Disproportionate destruction and/or loss of Life		

1	Weight assigned quantifiy importance
15	Resultant Equties Threshold

3

Immediacy

Is their sufficient time allowing the effect to develop and positively impact the operation?

For this mission, high score is a less desirable result.

Less likely to occur - more likely occur			Less likely to occur - more likely occur				Less likely to occur - more likely occur		
1	2	3	4	5	6	7	8	9	10
						1			

2	Weight assigned quantifiy importance
15	Resultant Equties Threshold

Result is instantaneous or can be instantiated at specified times as required	Result is predictable and has a specified time	The time is predictable, but the result is not.

14

Directness

Can the effect be attributed to the CNO?

For this mission, high score is a less desirable result.

High - Probability - Low							High - Probability - Low		High - Probability - Low
1	2	3	4	5	6	7	8	9	10
									1
Using multiple attack vectors, the effect can be attributed to CNO.			Using just the one attack vector, the effect can be attributed to CNO.				Using multiple attack vectors, the effect can be attributed to CNO or other means		

3	Weight assigned quantifiy importance
15	Resultant Equties Threshold

30	Danger

Invasiveness

What is the level of intrusiveness and will it cause a escalation of hostilities?

For this mission, high score is a less desirable result.

Less likely to occur - more likely occur			Less likely to occur - more likely occur				Less likely to occur - more likely occur		
1	2	3	4	5	6	7	8	9	10
		1							
Can be executed from the WAN or LAN without human intervention (i.e. .exe file) or force.			Accessible via WAN or LAN and use of force is already authorized and not required.				Accessible from direct human intervention or use of force and action likely to escalate hostilities.		

1	Weight assigned quantifiy importance
15	Resultant Equties Threshold

3

Measurability

What is the amount (monetarily/reconstruction/casualties) of damage caused by CNO?

For this mission, high score is a less desirable result.

Less - Benchmark - More			Less - Benchmark - More				Less - Benchmark - More		
1	2	3	4	5	6	7	8	9	10
						1			
Probable amount of damage.			Probable amount of damage.				Probable amount of damage.		

2	Weight assigned quantifiy importance
15	Resultant Equties Threshold

14

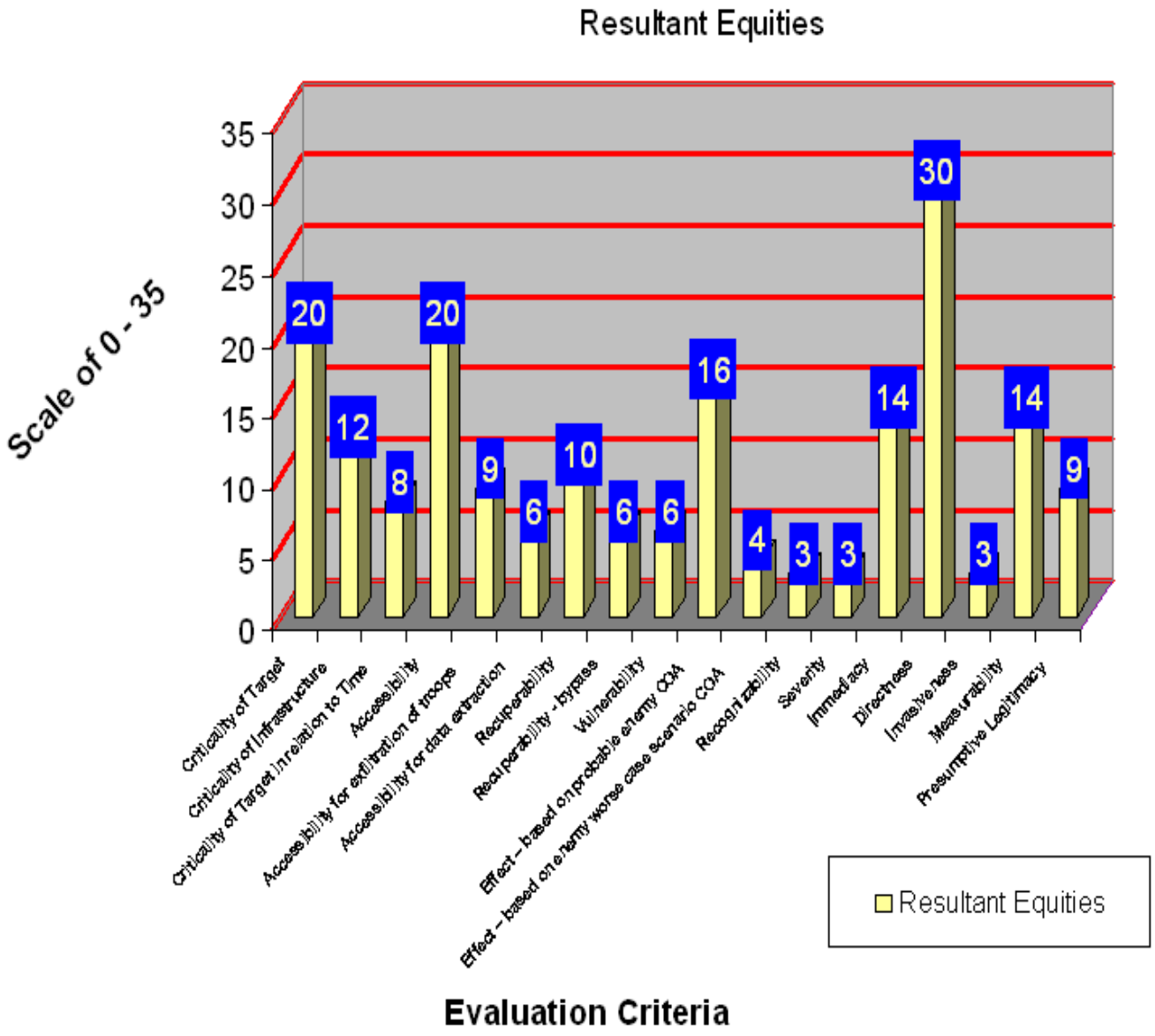
Presumptive Legitimacy

Is the tactic an acceptable response for the situation?

For this mission, high score is a less desirable result.

More - Acceptable - Less									More - Acceptable - Less			
1	2	3	4	5	6	7	8	9	10	3	Weight assigned quantifiy importance	
		1								15	Resultant Equties Threshold	9

Tactic has been used before and precedence is already established.	New weapon old tactic response is predictable.
	New tactic response uncertain.


Resultant Equities
Scale of 0 - 35
0
5
10
15
20
25
30
35
20
12
8
20
9
6
10
6
6
16
4
3
3
14
30
3
14
9
Criticality of Target
Criticality of Infrastructure
Criticality of Target in relation to Time
Accessibility
Accessibility for exfiltration of troops
Accessibility for data extraction
Recuperability
Recuperability - bypass
Vulnerability
Effect - based on probable enemy COA
Effect - based on enemy worse case scenario COA
Recognizability
Severity
Immediacy
Directness
Invasiveness
Measurability
Presumptive Legitimacy
Resultant Equities
Evaluation Criteria

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Chris Eagle
   Naval Postgraduate School
   Monterey, California

4. Dan C. Boger
   Naval Postgraduate School
   Monterey, California